

## **ANEXO I**

### **REQUISITOS TÉCNICOS DA SOLUÇÃO**

#### **1. ESCOPO GERAL DA SOLUÇÃO E MÓDULOS OBRIGATÓRIOS**

1.1. A solução contratada deverá incluir, nativamente integrados em uma única console e agente, no mínimo os seguintes módulos:

- 1.1.1. Anti-malware / NGAV multicamadas (assinaturas, heurística, comportamento e ML);
- 1.1.2. EDR com telemetria rica, busca (Threat Hunting), RCA e reconstrução de cadeias de ataque (kill-chain);
- 1.1.3. Firewall de endpoint e IPS de próxima geração com capacidade de virtual patching e bloqueio de explorações de rede;
- 1.1.4. Controle de aplicações (whitelisting/blacklisting por hash, caminho, certificado);
- 1.1.5. HIPS (Host-based Intrusion Prevention) e controles para proteção do SO (arquivos, chaves de registro, autorun, hosts);
- 1.1.6. Controle de dispositivos e DLP de endpoint com políticas granulares e inspeção de conteúdo;
- 1.1.7. Módulo especializado para proteção do Active Directory (detecção de abusos de Kerberos, movimentos laterais e mecanismos de deception);
- 1.1.8. Ferramentas de resposta remota (isolamento, execução remota de scripts, coleta forense, dump de memória) e automação por playbooks. (quando tecnicamente aplicável e suportado pelo SO e pelo fabricante, observando as políticas de privacidade e a LGPD).

#### **1.2. Requisitos do agente de endpoint**

- 1.2.1. Agente único e unificado: toda a funcionalidade essencial (EPP, EDR, DLP, HIPS, firewall, telemetria) deverá ser provida por um único agente sem dependência de agentes auxiliares para funcionalidades básicas.
- 1.2.2. Consumo e performance (valores mensuráveis exigidos):
  - Consumo médio de CPU em operação normal  $\leq 1\%$
  - Consumo médio de CPU durante varredura completa  $< 10\%$
  - Consumo médio de memória RAM em operação normal  $\leq 200$  MB
  - Consumo médio de memória durante atividades intensivas  $< 400$  MB
  - Tráfego de rede típico gerado pelo agente em operação normal  $< 100$  kbps
- 1.2.2.1. Poderão ser aceitos valores superiores aos exigidos acima, mediante justificativa da contratada sujeita à análise do MCOM, desde que comprovada baixa interferência no desempenho do endpoint.
- 1.2.3. Autoproteção (anti-tampering): o agente deve resistir a tentativas de desativação, modificação ou remoção não autorizada; a desinstalação só poderá ser efetuada mediante credenciais da console e processo protegido por autenticação forte (MFA). Caso o console dependa de IdP externo, o fabricante deverá comprovar que o fluxo garante MFA em todos os caminhos administrativos (ou prover MFA nativo).
- 1.2.4. Operação offline: o agente deve manter as últimas políticas e operar por, no mínimo, 30 dias sem conectividade com o console, executando controles DLP e políticas locais.
- 1.2.5. Atualizações e distribuição de assinaturas/engine: o agente e o console devem suportar atualização incremental automática (mínimo diário) das definições/engine, e haver opção de distribuir atualizações via servidores internos ou clientes eleitos (peer distribution) com controle de banda, sem necessidade de reinicialização obrigatória para aplicar as definições.

- 1.2.6. Requisitos de compatibilidade: o agente deve suportar versões e edições de Windows (estações e servidores) e Linux (principais distribuições corporativas), devendo o fornecedor declarar compatibilidade e limitações expressas na proposta técnica.

### **1.3. Console de gerenciamento central**

- 1.3.1. Arquitetura e certificações: console de gerenciamento central (plataforma SaaS) hospedada em nuvem segura com certificações ISO 27001 (ou equivalente) e SOC 2 Tipo II (ou equivalente); SLA de disponibilidade contratual mínimo 99,95%.
- 1.3.2. Acesso e autenticação: acesso via HTTPS/TLS 1.2+; interface nativa em Português-BR; suporte a SAML 2.0, LDAP/AD, OAuth/OIDC para integração de identidade; MFA obrigatória para administradores; possibilidade de restrição por ranges de IP. Quando o console tiver retenção limitada de logs (ex.: 30 dias), deverá comprovar integração e entrega ao SIEM do CONTRATANTE para manter retenção de 1 ano.
- 1.3.3. RBAC e auditoria: Controle de Acesso Baseado em Função (RBAC) granular; perfis predefinidos e customizáveis; trilha de auditoria imutável com retenção mínima de 1 ano (ou exportação automática para repositório do CONTRATANTE).
- 1.3.4. Gerenciamento de políticas e grupos: organização de endpoints em grupos dinâmicos e estáticos; aplicação de políticas por atributos (usuário, OU AD, tags, rede, localização); implantação remota e agendada de agentes; mecanismos de rollback e versionamento de políticas.
- 1.3.5. Dashboards e relatórios: dashboards em tempo real; relatórios customizáveis; suporte a exportação (CSV, JSON) e integração via APIs com SIEM/SOAR.
- 1.3.6. Requisitos de integração: APIs REST bem documentadas, webhooks, syslog e conectores pré-construídos para SIEM/CMDB/ITSM.

### **1.4. EPP / NGAV**

- 1.4.1. Proteção em tempo real (on-access): motor que combine assinaturas, heurística, análise comportamental e Machine Learning com atualização contínua de reputação.
- 1.4.2. Proteção fileless e scripts: detecção e bloqueio de técnicas sem arquivo, incluindo execução via PowerShell, WMI, macros e interpreters; capacidade de analisar comportamento em memória.
- 1.4.3. Verificação e tratamento de arquivos compactados recursivamente (suporte mínimo a 10 níveis de compactação) e análise de arquivos grandes (>20MB) conforme necessidades documentadas.
- 1.4.4. Ações configuráveis por categoria: permitir a definição de ações primárias e secundárias (alertar, limpar, quarentenar, apagar) por categoria de ameaça; lista de exclusões com níveis de severidade e impacto.
- 1.4.5. Capacidade de reversão: possibilidade de restaurar assinaturas/definições anteriores armazenadas no servidor (rollback de vacina).
- 1.4.6. Requisitos operacionais: suporte a planos de distribuição de atualizações, escolha de clientes para distribuição e controle de banda.

### **1.5. EDR - telemetria, hunting e resposta**

- 1.5.1. Coleta de telemetria: coleta contínua e em tempo real de processos, rede, filesystem, registro, eventos de autenticação, carregamento de bibliotecas, linhas de comando e outros artefatos relevantes.
- 1.5.2. Retenção e pesquisa: telemetria online pesquisável por período mínimo de 90 dias (dados críticos) e possibilidade de exportação para análise histórica.
- 1.5.3. Mapeamento MITRE ATT&CK: todos os alertas e eventos devem ser mapeados ao framework MITRE ATT&CK com visualização interativa.

- 1.5.4. Threat Hunting: interface com linguagem de consulta avançada (query language) para buscas proativas; suporte a consultas ad-hoc e saved searches.
- 1.5.5. RCA e reconstrução de cadeia de ataque: geração automática de árvores correlacionadas (causa raiz, origem, propagação, artefatos e timeline).
- 1.5.6. Ações remotas e orquestração: isolamento de rede (modo 'seguro' permitindo apenas comunicação com o console), finalização de processos, quarentena/deleção de arquivos, modificação de chaves de registro, parada de serviços, reboot, execução remota de scripts (PowerShell/Bash) com log de output.
- 1.5.7. Coleta forense remota: coleta de arquivos, logs e dump de memória para análise forense com mecanismo de exportação segura. (quando tecnicamente aplicável e suportado pelo SO e pelo fabricante, observando as políticas de privacidade e a LGPD).
- 1.5.8. Automação (playbooks): criação de playbooks condicionais que executem sequências de ações baseadas em gatilhos, com versionamento e testes em ambiente controlado.

#### **1.6. Proteção contra exploração de memória**

- 1.6.1. Cobertura mínima: mitigar explorações em aplicações críticas (navegadores, runtime Java, pacotes Office, ambientes .NET e aplicações corporativas críticas).
- 1.6.2. Detectar e bloquear shellcode, técnicas de injeção de código e exploração baseada em memória, com alerta detalhado indicando processo, PID, caminho, hash, linha de comando e processo pai.
- 1.6.3. Permitir configuração de sensibilidade e tuning por aplicação e grupos de endpoints.

#### **1.7. Hardening, controle de aplicações e exceções**

- 1.7.1. Application Control: repositórios de aplicações confiáveis; suporte a whitelisting/blacklisting por hash (MD5/SHA1/SHA256), caminho, fabricante e certificado digital.
- 1.7.2. Descoberta e catálogo: descoberta automática de aplicações instaladas para auxiliar na criação de políticas.
- 1.7.3. Trusted Updaters: definição de processos/atualizadores confiáveis (Windows Update, SVCHost, instaladores corporativos) com política de exceção.
- 1.7.4. Modo de simulação/auditoria: políticas aplicáveis em modo 'monitor' para avaliar impacto; workflow de solicitações de exceção com justificativa e aprovação registrada (audit trail).
- 1.7.5. Application hardening: bloquear execução de aplicações não autorizadas mesmo com privilégios administrativos.

#### **1.8. Redução da superfície de ataque e LOTL**

- 1.8.1. Detecção contextual de LOTL: distinguir uso legítimo vs malicioso de ferramentas administrativas (PowerShell, psexec, WMIC, etc.) levando em conta usuário, processo pai, argumentos e comportamento subsequente.
- 1.8.2. Base de referência LOTL: oferecer base mínima de aplicações conhecidas (Ponto 1 exige referência mínima de 50 aplicações) e mapear cada comportamento ao MITRE ATT&CK.
- 1.8.3. Auto-tune e prevalência: capacidade de auto-sintonização com histórico de prevalência de comportamento por, no mínimo, 6 meses; geração automática de recomendações e exceções.
- 1.8.4. Isolamento de aplicações não confiáveis: política de isolamento que impede exclusão/modificação de arquivos e pastas críticas, com modo de simulação e logs detalhados.

#### **1.9. Controle de dispositivos e DLP**

- 1.9.1. Controle granular de dispositivos USB: políticas por tipo, classe, fabricante, modelo e número de série; suporte à exceção por número de série; operações de leitura/escrita/execução configuráveis.

- 1.9.2. Controle de outras interfaces: Wi-Fi, Bluetooth, portas seriais, FireWire, CD/DVD, etc.
- 1.9.3. Políticas baseadas em localização e contexto: permitir políticas diferenciadas dependendo da rede, VLAN, OU do AD ou tag de inventário.
- 1.9.4. DLP de endpoint — requisitos operacionais e de capacidade (lista exaustiva extraída do Ponto 1):
  - 1.9.4.1. Identificação de dados sensíveis por palavras-chave, regex e dicionários (CPF, CNPJ, números bancários, RG, título de eleitor, endereços IP etc.);
  - 1.9.4.2. Impressão digital de documentos estruturados e não estruturados (docx, pdf, planilhas, CAD, código-fonte, diagramas);
  - 1.9.4.3. Detecção por similaridade configurável: parâmetro percentual configurável por política; criação automática de incidentes quando limiar for atingido;
  - 1.9.4.4. Suporte a verificação de arquivos compactados recursivos (.zip, .rar, .7z) e análise de arquivos grandes (>20 MB);
  - 1.9.4.5. Detecção em Português-BR comprovada (o fornecedor deverá apresentar evidência de eficácia para PT-BR);
  - 1.9.4.6. Inspeção de conteúdo em colunas de planilhas e campos de bancos de dados (quando aplicável);
  - 1.9.4.7. Ações automáticas configuráveis sem necessidade de scripts externos: quarentena, bloqueio de upload, bloqueio de impressão, bloqueio de cópia para USB, bloqueio de transferência para compartilhamento de rede, bloqueio de protocolos (FTP/HTTP/HTTPS/SMTP), envio de incidente via syslog, notificação a usuário e gestores, adição de atributos e alteração de status;
  - 1.9.4.8. Interface nativa de orquestração de resposta (combinação de ações) com auditoria;
  - 1.9.4.9. Armazenamento em cache local dos arquivos que causaram incidente até reconexão ao ambiente corporativo;
  - 1.9.4.10. Monitoramento e bloqueio de clipboard (copiar/colar) e captura de tela;
  - 1.9.4.11. Monitoramento de clientes de e-mail (ex.: Outlook) e bloqueio de envios indevidos;
  - 1.9.4.12. Capacidade de gerar notificações por e-mail customizáveis com seleção de informações do incidente a serem enviadas.

#### **1.10. Proteção e resposta ao Active Directory (AD)**

- 1.10.1. Detecção de ataques a credenciais: identificação de Kerberoasting, Pass-the-Hash, Pass-the-Ticket, Overpass-the-Hash, Forged PAC, DCSync, Golden Tickets e enumeração de sessão.
- 1.10.2. Monitoramento AD sem dependência exclusiva de agentes em DCs: a solução deve correlacionar sinais de endpoints para detectar anomalias no AD quando aplicável.
- 1.10.3. Deception e mascaramento de topologia: preferencialmente mecanismo nativo para implantar decoys (usuários/computadores) e mascarar topologia; caso não seja disponibilizado nativamente, aceitar integração com solução especializada.
- 1.10.4. Resposta automatizada no AD: ação com um clique para forçar redefinição de senha, invalidação de sessões e geração de relatório de avaliação de vulnerabilidades.

#### **1.11. Não-funcionais: desempenho, escalabilidade e latência (exigências)**

- 1.11.1. Capacidade: suportar, em modo SaaS, gerenciamento de, no mínimo, 1.200 endpoints sem degradação; arquitetura escalável para 5.000 endpoints.
- 1.11.2. Latências máximas (SLAs técnicos): propagação de políticas ≤ 5 minutos; envio de telemetria crítica ≤ 30 segundos; execução de ações remotas (ex.: isolamento) ≤ 10 segundos.

- 1.11.3. Disponibilidade e resiliência: SLA da plataforma de 99,95% com planos de contingência e continuidade.

#### **1.12. Segurança da solução e cadeia de suprimentos (SDLC e evidências)**

- 1.12.1. Certificações: o fabricante deve demonstrar conformidade com padrões (ISO 27001 ou equivalente, SOC 2 Tipo II ou equivalente) e políticas de segurança da cadeia de suprimentos.
- 1.12.2. SDLC e práticas de desenvolvimento seguro: o fornecedor deve apresentar documentação do SDLC, políticas de secure coding, resultados de testes de segurança (pen tests, SAST/DAST), e gestão de vulnerabilidades com prazos de correção e CVE tracking. A não comprovação das práticas de desenvolvimento seguro, conforme exigido, resultará na desclassificação da proposta.
- 1.12.3. Auditoria e acesso a evidências: obrigação de fornecer evidências e permitir auditoria técnica (POC, logs, relatórios) mediante solicitação justificada.

#### **1.13. Integrações, exportação de dados e formatos**

- 1.13.1. APIs: APIs REST/JSON bem documentadas e estáveis; suporte a autenticação via tokens/credentials com rotação e expiração.
- 1.13.2. Exportação: suporte a exportações em CSV e JSON; integração via syslog e conectores para SIEM e SOAR.
- 1.13.3. Conectores: conectores pré-construídos para os principais SIEMs do mercado, com playbooks de ingestão e normalização.