INSTITUTO NACIONAL DO SEGURO SOCIAL

ESPECIFICAÇÃO TÉCNICA

Objeto
Subscrição de licenças de softwares para Solução de Segurança Integrada de Proteção Avançada de Endpoints (estações de trabalho e servidores de rede) e Detecção e Resposta de Endpoint (Endpoint Detection and Response - EDR), incluindo capacitação e serviço especializado de implantação.

Detalhamentos dos Itens do Objeto

Características Gerais

1 As licenças devem ser disponibilizadas por meio de subscrição e devem estar plenamente ativas até 90 dias após o término do contrato;

2 Capacidade de remover remotamente e automaticamente, de forma nativa ou com uso de scripts, qualquer solução de segurança (própria ou de terceiros) que estiver presente nas estações e servidores;

3 Capacidade de instalar remotamente a solução de segurança nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;

4 Deve registrar em arquivo de *log* todas as atividades efetuadas pela solução e deve enviar também essas informações para a console de gerência centralizada da solução;

5 Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto;

6 A comunicação de rede entre o cliente e o servidor de administração deve ser criptografada;

7 Integração com serviços de diretórios da solução Microsoft Active Directory ou OpenLDAP;

8 Todas as funcionalidades dos módulos especificados devem ser, conforme requisitos de implantação da solução, ser plenamente compatíveis com as seguintes versões de sistemas operacionais:

a) *Endpoints* Windows 7 ou superior e servidores Windows Server 2019 ou superior; e

b) Servidores Debian 11 ou superior e Ubuntu 20 LTS ou superior, que serão abrangidos pelas licenças contratadas por meio de ordens de serviço posteriores à implantação inicial a serem executadas, sob demanda, conforme entregas do projeto de atualização interna das versões dos sistemas operacionais, ou distribuições GNU/Linux no geral;

ESPECIFICAÇÃO TÉCNICA

Objeto
Subscrição de licenças de softwares para Solução de Segurança Integrada de Proteção Avançada de Endpoints (estações de trabalho e servidores de rede) e Detecção e Resposta de Endpoint (Endpoint Detection and Response - EDR), incluindo capacitação e serviço especializado de implantação.

9 O licitante vencedor deverá fornecer todos os softwares auxiliares necessários para o funcionamento da solução e sem custo adicional;

10 A solução e seus softwares auxiliares, que estejam implantados localmente, devem continuar funcionando após o término do contrato com as últimas atualizações baixadas antes do encerramento do contrato;

11 Não será permitido o envio de arquivos, links, endereços e quaisquer outras informações proprietárias do INSS para a nuvem. Será permitido apenas o tráfego de dados e metadados imprescindíveis para o funcionamento da solução;

12 Qualquer módulo da solução que tenha de ser necessariamente hospedado ou que tenha de usar recursos em nuvem deve satisfazer os requisitos mínimos de segurança da informação definidos pela INSTRUÇÃO NORMATIVA Nº 5 DO GSI, DE 30 DE AGOSTO DE 2021;

13 A solução deve ser capaz de gerenciar o agendamento de atualizações e instalações de políticas e agentes;

14 Qualquer adaptação ou configuração das funcionalidades dos módulos especificados da solução que precisem, por ventura, se integrar com soluções externas deve ser realizada de forma nativa;

15 Todas as funcionalidades dos módulos especificados devem ser otimizadas, adaptativa ou manualmente, para *endpoints* e servidores com poucos recursos computacionais (CPU, RAM e disco) de modo a não comprometer a utilização do ativo protegido;

16 Todos os módulos auxiliares imprescindíveis ao funcionamento da console de gerenciamento devem ser implementados em alta disponibilidade.

1)Solução de Proteção de computadores

1.1 A solução de gerência centralizada deve:

ESPECIFICAÇÃO TÉCNICA

Objeto
Subscrição de licenças de softwares para Solução de Segurança Integrada de Proteção Avançada de Endpoints (estações de trabalho e servidores de rede) e Detecção e Resposta de Endpoint (Endpoint Detection and Response - EDR), incluindo capacitação e serviço especializado de implantação.

1.1.1 permitir a geração de relatórios, visualizar eventos, gerenciar políticas e, se possível, a criação de painéis de controle customizados;

1.1.2 permitir, de forma nativa ou por meio da utilização de scripts, a visualização da situação, dos recursos instalados (CPU, memória, discos, conexões de rede, dentre outros), softwares instalados, em tempo real, de todos os ativos administrados pela console de gerenciamento centralizada;

1.1.3 gerenciar estações de trabalho, servidores de rede e servidores de arquivos protegidos pela solução de segurança;

1.1.4 ser capaz de importar a estrutura da solução Microsoft Active Directory para descoberta de máquinas;

1.1.5 permitir, por meio da console de gerenciamento, a criação de políticas para a retenção em servidor de rede de arquivos que violam as políticas de segurança definidas para os ativos abrangidos pela solução;

1.1.6 monitorar diferentes sub-redes a fim de encontrar máquinas novas para serem adicionadas à proteção, para soluções em nuvem será aceito o uso do Microsoft Active Directory, scripts ou outras ferramentas para executar tal função;

1.1.7 monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;

1.1.8 ser capaz de, assim que detectar máquinas novas, nativamente ou através de Script nos diretórios da solução Microsoft Active Directory, sub-redes ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possua, deve instalar o antivírus automaticamente;

1.1.9 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;

1.1.10 fornecer, de forma nativa ou por meio da exportação de relatório, as seguintes informações dos ativos protegidos:

Objeto
Subscrição de licenças de softwares para Solução de Segurança Integrada de Proteção Avançada de Endpoints (estações de trabalho e servidores de rede) e Detecção e Resposta de Endpoint (Endpoint Detection and Response - EDR), incluindo capacitação e serviço especializado de implantação.

a) Quais módulos de segurança estão instalados;

b) Quais módulos de segurança estão com o serviço iniciado;

c) Quais módulos de segurança estão atualizados;

d) Minutos/horas desde a última conexão do ativo com o servidor administrativo;

e) Minutos/horas desde a última atualização;

f) Data e horário da última varredura executada no ativo;

g) Versão dos módulos de segurança instalados no ativo;

h) Quantidade de ameaças identificadas no ativo;

i) Nome do ativo;

j) Domínio ou grupo de trabalho do ativo;

k) Sistema operacional;

l) Endereço IP;

m) Eventos de segurança relacionados aos aplicativos instalados no ativo;

n) Informações sobre incidentes no painel central.

1.1.11 exportar relatórios, de forma nativa ou por meio de API, para os tipos de arquivos PDF e HTML e, opcionalmente, para os tipos de arquivos XML, CSV e JSON.

1.1.12 gerar, de forma preferencial, *traps* SNMP para monitoramento de eventos.

1.1.13 enviar e-mails para contas específicas em caso de algum evento específico.

1.1.14 realizar atualização incremental da base de assinatura de malware.

1.1.15 realizar a atualização incremental das bases de reputação.

1.1.16 reportar vulnerabilidades de softwares presentes nos ativos ou possuir mecanismos de proteção contra exploração de vulnerabilidades.

1.1.17 disponibilizar a criação de perfis e papéis de acesso. Exemplo: Administradores, operadores, monitores.

1.1.18 ser capaz de se integrar com a solução Microsoft Active Directory ou serviço de diretório OpenLDAP para a autenticação no painel central de gerência.

1.1.19 ser capaz de gerar relatório forense detalhando o modus operandi de cada malware identificado e informar qual foi o vetor de contaminação/entrada em cada ocorrência.

1.1.20 possuir console única de visibilidade e de consolidação de gerenciamento integrado do ambiente monitorado por múltiplos ativos (*endpoints*, servidores e dispositivos).

1.1.22 possuir integração com *syslog*.

1.1.23 possuir integração com soluções SIEM ou SOAR.

1.1.23 ser capaz de desativar temporariamente funcionalidades da solução, quando necessário para efeitos de suporte, localmente, mas protegida com senha.

1.1.24 ser capaz de gerenciar o envio de alertas e notificações.

1.1.25 centralizar a gerência de todos os recursos e funcionalidades especificadas.

1.1.26 permitir o agendamento e envio de relatórios por email.

1.1.27 permitir a criação de relatórios customizados.

1.1.28 possuir modelos predefinidos de relatórios de forma a facilitar a geração de relatórios

1.1.30 ser capaz de criptografar toda comunicação entre o painel de gerenciamento e a solução.

1.1.31 ser gerenciada totalmente por console web.

1.2 A solução de Proteção de Computadores:

1.2.1 deve possuir as seguintes características e funcionalidades:

1.2.1.1 ser capaz de atualizar os pacotes de instalação com as últimas vacinas;

Objeto
Subscrição de licenças de softwares para Solução de Segurança Integrada de Proteção Avançada de Endpoints (estações de trabalho e servidores de rede) e Detecção e Resposta de Endpoint (Endpoint Detection and Response - EDR), incluindo capacitação e serviço especializado de implantação.

1.2.1.2 ser capaz de identificar e bloquear, no mínimo, os seguintes tipos de malwares: ameaças de dia zero (*zero-day*), direcionado, *ransomware*, *spyware*, *worm*, *adware*, *bot(nets)*, *rootkits*, *trojan*, *fileless virus*, vírus.

1.2.1.3 ser capaz de, no mínimo, identificar artefatos maliciosos por meio das seguintes técnicas: análise baseada em assinaturas, análise baseada em reputação (*hashes* de Indicadores de Comprometimento) *machine learning* com pré-execução, análise comportamental, análise heurística, mecanismo de emulação, mecanismo de inteligência artificial, análise de comunicações de rede.

1.2.1.4 possuir os seguintes módulos de segurança:

a) firewall;

b) IPS;

c) proteção de navegadores web;

d) controle de aplicação;

e) filtro de reputação web;

f) controle de dispositivos;

g) detecção e reposta para computadores (*endpoint detection and response* - EDR);

h) proteção de memória;

i) proteção *anti-malware* para computadores com GNU/Linux;

j) aplicação de políticas e mecanismos de segurança que alertem e protejam contra ameaças a vulnerabilidades em sistemas operacionais e nas aplicações instaladas;

1.2.1.5 ser dotada de um módulo de controle de aplicação com as seguintes características:

1.2.1.5.1 possibilitar a criação de política de bloqueio de execução de aplicações por: nome de arquivo ou diretório ou *hash*;

1.2.1.5.2 possibilitar a criação de política para a liberação de aplicações assinadas por uma autoridade certificadora raiz confiável. A ferramenta deverá possuir uma relação prévia de autoridades certificadoras confiáveis e o INSS ou Dataprev poderão importar as suas;

1.2.1.5.3 possibilitar a liberação e bloqueio de aplicações por meio de *white list* e *black list* de aplicações;

1.2.1.5.4 aplicar o controle de aplicação em tempo de execução;

1.2.1.5.5 monitorar alterações em arquivos e chaves de registro em tempo real e possuir mecanismos de proteção;

1.2.1.5.6 possuir proteção contra adulteração de programas (executáveis, binários, DLLs, *scripts*, etc);

1.2.1.5.7 possibilitar a criação de políticas para computadores específicos, onde somente será permitido executar programas autorizados (*white list*) ou serão bloqueados os programas não autorizados (*black list*);

na lista de bloqueio via política de controle de aplicação;

1.2.1.5.8 ser capaz de permitir e bloquear a instalação e a execução de programas específicos, categorias de programas (no caso de *endpoints*), de acordo com política definida pelo INSS;

1.2.1.5.9 analisar as ações de cada aplicação em execução no *endpoint* ou servidor, gravando tais ações executadas e comparando-as com sequências características de atividades suspeitas ou perigosas;

1.2.1.10 analisar qualquer tentativa de edição, exclusão ou gravação do registro do Windows ou de arquivos de configuração em distribuições GNU/Linux antes de sugerir ações e bloquear comportamentos suspeitos e perigosos;

1.2.1.6 ser dotada de um módulo de controle de dispositivos com as seguintes características:

ESPECIFICAÇÃO TÉCNICA

Objeto
Subscrição de licenças de softwares para Solução de Segurança Integrada de Proteção Avançada de Endpoints (estações de trabalho e servidores de rede) e Detecção e Resposta de Endpoint (Endpoint Detection and Response - EDR), incluindo capacitação e serviço especializado de implantação.

1.2.1.6.1 capaz de controlar a utilização de dispositivos removíveis permitindo a identificação e o controle de leitura, escrita e execução. Os seguintes padrões de portas físicas devem ser suportados: USB, *Thunderbolt*, *Firewire*, CD/DVD, SD Card, eSATA e micro USB;

1.2.1.6.2 ser capaz de identificar, permitir e bloquear a utilização de dispositivos acoplados nos ativos protegidos pela solução;

1.2.1.6.3 ser capaz de identificar e impedir movimentos laterais suspeitos e maliciosos por meio do isolamento do equipamento gerenciado;

1.2.1.7 verificar a confiabilidade dos executáveis e caso não seja confiável, deverá possuir capacidade para impedir sua execução.

1.2.1.8 ser capaz de bloquear a execução de executáveis em geral em dispositivos removíveis.

1.2.1.9 ser capaz de verificar a integridade de arquivos do sistema operacional e de programas instalados.

1.2.1.10 ser capaz de registrar na base de reputação os novos malwares identificados.

1.2.1.11 ser dotada de um módulo de proteção de memória capaz de identificar e bloquear ações maliciosas realizadas por softwares permitidos. Exemplo: execução de *shellcodes*, comandos, ações com privilégios elevados, etc.

1.2.1.12 capaz de remover arquivos maliciosos automaticamente.

1.2.1.13 ser capaz, caso possua funcionalidade de quarentena local, de mover arquivos suspeitos para área protegida no computador ou tomar alguma ação de mitigação de tais arquivos, de acordo com a definição em política.

1.2.1.14 ser capaz de mover, caso possua funcionalidade de quarentena local, arquivos maliciosos para servidor de rede de acordo com a definição em política ou permitir a recuperação do arquivo no computador por meio da console de gerenciamento centralizada.

1.2.1.15 ser capaz de tratar exceções, evitando o bloqueio e até mesmo a verificação de processos, diretórios e executáveis especificados em políticas.

1.2.1.16 ser capaz de se integrar com sistemas SIEM ou SOAR externos.

1.2.1.17 ser capaz de detectar a presença de soluções de proteção de computadores de outro fabricante que possa causar incompatibilidade.

1.2.1.18 ser dotada de um módulo de proteção de navegação web capaz de verificar tráfego nos browsers mais utilizados no mercado executando bloqueio por reputação ou categorização do URL.

1.2.1.19 ser dotada de um módulo de filtro de conteúdo web capaz de adicionar sites da web em uma lista de exclusão (*black list*) e em uma lista de permissão (*white list*).

1.2.1.20 ser dotada de proteção contra desinstalação por meio de senha.

1.2.1.21 ser dotada de um módulo de firewall para *endpoints* e servidores gerenciado a partir da console de gerência centralizada, com filtragem de pacotes e de aplicativos;

1.2.1.22 utilizar um agente único nos *endpoints* e servidores, de modo a atender todas as funcionalidades, não sendo permitido o uso de agentes simultâneos no mesmo ativo.

1.2.1.23 ser dotada de um módulo de proteção contra *ransomware* capaz de desfazer quaisquer alterações criptográficas nos arquivos dos *endpoints* e servidores.

2)Solução de Detecção e Resposta de Ameaças contra computadores

2.1 O módulo de *Endpoint Detection and Response* (EDR) deve possuir as seguintes características:

2.1.1 possibilitar a investigação nos *endpoints* Windows e servidores GNU/Linux via console de gerenciamento, por meio de consultas customizadas que serão realizadas em todos os computadores com o módulo ativado;

2.1.2 possibilitar a detecção e identificação de atividades suspeitas em todos os computados com o módulo ativado;

2.1.3 gerar trilha de auditoria dos eventos nos computadores com o módulo ativo. As informações de auditoria devem conter, no mínimo:

a) informações sobre processos: criados, finalizados, *hash* SHA-1, ID, *Time*, *User,* comando que iniciou o processo, RAM utilizada pelo processo e *Threads* criados pelo processo, registros e bibliotecas alteradas,

b) informações sobre conexões de rede: endereço IP de origem e destino, portas de origem e destino;

c) informações sobre arquivos: nome do arquivo, data de criação, data de modificação e data de exclusão;

d) informações sobre registros de sistema: nomes de chaves e valores correspondentes. Os valores deverão constar nos registros;

e) informações sobre Sistema Operacional: versão, grupo de usuários locais, membros de grupos de usuários locais e usuários locais.

2.1.4 consultas à trilha de auditoria via console de gerenciamento centralizada;

2.1.5 permitir a execução de scripts (PowerShell, VisualBasic, BAT ou Python em computadores Windows e ShellScript ou Python em servidores GNU/Linux) ou de ações pré-definidas e customizáveis (no mínimo: isolar o host, verificar IoC's e isolar ou prevenir a execução de arquivos);

2.1.7 possuir políticas pré-configuradas;

2.1.8 permitir a criação de coletores de informações e a execução de scripts sob demanda em computadores;

2.1.9 armazenar os eventos nos computadores e disponibilizar consulta a eles via console de gerenciamento.