SECRETARIA DE ADMINISTRAÇÃO DO ESTADO DO PIAUÍ
Av. Pedro Freitas, 1900, Centro Administrativo, BL1 - Bairro São Pedro, Teresina/PI, CEP 64018-900
Telefone: - http://www.sead.pi.gov.br/

ESTUDO TÉCNICO PRELIMINAR ETP Nº: 15 /SEAD-PI/GAB/NTGD/GIS TERESINA/PI, 21 DE MAIO DE 2025.

Processo nº 00002.012947/2023-48

SECRETARIA DA ADMINISTRAÇÃO - SEAD

GOVERNO DO PIAUÍ
AQUI TEM TRABALHO.
AQUI TEM FUTURO.

ESTUDO TÉCNICO PRELIMINAR

Processo Administrativo nº 00002.012947/2023-48

REGISTRO DE PREÇOS PARA CONTRATAÇÃO DE EMPRESA PARA FORNECIMENTO, SOB DEMANDA, DE SOLUÇÃO DE SEGURANÇA PARA PROTEÇÃO DE E-MAIL, ENDPOINT E PROTEÇÃO CONTRA ATAQUES AVANÇADOS, INCLUINDO INSTALAÇÃO, CONFIGURAÇÃO, REPASSE DE CONHECIMENTO, SUPORTE TÉCNICO E GARANTIA,
PARA ATENDER ÀS NECESSIDADES DOS ÓRGÃOS E ENTES DA ADMINISTRAÇÃO PÚBLICA, PELO PERÍODO DE 24 MESES,

CONFORME ESPECIFICAÇÕES E QUANTIDADES PREVISTAS NO TERMO DE REFERÊNCIA.

Teresina, Março de 2024

Histórico de Revisões

Data	Versão	Descrição	Autor
05/03/2024	1.0	Finalização da primeira versão do documento	Adriano Moura Macedo Ubaldo de Sá Neves Júnior
10/12/2024	2.0	Finalização da segunda versão do documento	Adriano Moura Macedo Ubaldo de Sá Neves Júnior
02/06/2025	3.0	Finalização da terceira versão do documento	Adriano Moura Macedo Ubaldo de Sá Neves Júnior

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

1. INTRODUÇÃO

1.1. O Estudo Técnico Preliminar – ETP é o documento constitutivo da primeira etapa do planejamento de uma contratação, que caracteriza o interesse público envolvido e a sua melhor solução. Ele serve de base ao Termo de Referência a ser elaborado, caso se conclua pela viabilidade da contratação.

1.2. O ETP tem por objetivo identificar e analisar os cenários para o atendimento de demanda registrada no Documento de Formalização da Demanda – DFD, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar a tomada de decisão e o prosseguimento do respectivo processo de contratação.

1.3. Referência: Inciso XI, do art. 2º e art. 11 da IN SGD/ME nº 94/2022.

2. DESCRIÇÃO DA NECESSIDADE

2.1. A segurança da rede da Secretaria de Estado de Administração e Previdência – SEAD-PI depende da utilização de recursos de segurança cibernética, que incluem várias camadas de proteção para monitorar o comportamento dos usuários, estações de trabalho e caixas postais com o objetivo de proteger o ambiente da Secretaria contra ameaças básicas e avançadas.

2.2. É fundamental tratar a informação como um recurso estratégico e econômico, devido à crescente valorização dos dados pessoais e da informação como ativos de gestão do Estado. Além disso, considerando as transações bilaterais cada vez mais frequentes que contam com o suporte de TI. O uso inadequado desses recursos oferece um alto risco de impactos negativos e pode resultar em consequências indesejadas, como prejuízo financeiro, problemas operacionais, danos à imagem do órgão ou governo, vazamento de informações e dados pessoais, e até mesmo sequestro de dados.

2.3. A SEAD-PI possui um parque computacional para atendimento aos usuários, com cerca de 2.000 usuários ativos na rede, 1.200 estações de trabalho, além de caixas postais e outros recursos, de acordo com o levantamento realizado no ambiente de infraestrutura de TI. A aferição do comportamento das estações de usuários e caixas postais tem como objetivo detectar, bloquear, investigar e responder a incidentes de segurança da informação que possam ocorrer na rede da Secretaria.

2.4. É essencial garantir a proteção e a integridade dos dados e sistemas da SEAD-PI, bem como a segurança dos usuários e da informação compartilhada. Portanto, é necessário implementar medidas de monitoramento contínuo, análise de logs, detecção de anomalias e resposta rápida a incidentes, a fim de mitigar riscos e garantir um ambiente seguro e confiável para as operações da Secretaria.

2.5. De acordo com estatísticas recentes do CERT.br, que recebe notificações de CSIRTs, administradores de redes e usuários de Internet, tem havido um aumento significativo nos ataques e incidentes de segurança ao longo dos anos. Especificamente, em 2022, foram notificados 481.652 incidentes ao CERT.br, um número alarmante. No entanto, é ainda mais preocupante que, apenas no primeiro semestre de 2023, esse número já tenha atingido 333.905 notificações, representando um aumento expressivo em relação ao período anterior.

2.6. Esses dados evidenciam uma tendência preocupante e urgente, que exige a adoção de medidas cada vez mais eficientes por parte das organizações. A segurança das informações e a proteção de dados pessoais tornaram-se questões críticas e de extrema importância, tanto para empresas quanto para indivíduos. É necessário que as organizações estejam preparadas para enfrentar e responder a esses incidentes de forma adequada, protegendo tanto os dados de sua propriedade quanto aqueles que estão sob sua custódia.

2.7. Diante desse cenário, é fundamental investir em estratégias robustas de segurança da informação, incluindo a implementação de sistemas de detecção e prevenção de ameaças, atualizações regulares de software e hardware, treinamento e conscientização dos usuários, além de políticas de segurança claras e bem definidas. Além disso, é importante contar com equipes especializadas em segurança cibernética, capazes de identificar e responder rapidamente aos incidentes, minimizando danos e prejuízos.

2.8. A proteção dos dados pessoais e a segurança das informações são responsabilidades compartilhadas, exigindo a colaboração de todos os usuários e organizações. É essencial promover uma cultura de segurança, estimulando a adoção de boas práticas e a conscientização sobre os riscos existentes. Somente assim poderemos enfrentar os desafios cada vez mais frequentes e sofisticados no mundo da segurança cibernética e garantir a integridade e confidencialidade dos dados de forma eficaz.

2.9. Portanto, é crucial fornecer à SEAD-PI recursos de segurança atualizados, capazes de monitorar e responder a infecções causadas por software malicioso desenvolvido por indivíduos com más intenções. Esses recursos abrangem desde a exposição simples de informações obtidas até a exigência de pagamento de resgate para a liberação de dados sequestrados, como ocorre nos ataques de ransomware. Além disso, é essencial que esses recursos garantam a detecção proativa de ameaças, a implementação de medidas preventivas, a resposta rápida a incidentes e a recuperação eficiente dos sistemas afetados.

2.10. Dessa forma, a contratação de recursos adicionais para cumprir com a LGPD é uma medida indispensável para garantir a proteção e preservar a privacidade dos usuários da SEAD-PI. Ao implementar as medidas de proteção adequadas, a secretaria estará em conformidade com a legislação vigente, assegurando a confidencialidade, integridade e disponibilidade dos dados pessoais sob sua responsabilidade.

3. NECESSIDADES DE NEGÓCIO

3.1. A contratação em questão tem como objetivo atender às necessidades de segurança da SEAD-PI, garantindo o cumprimento das diretrizes da Lei Geral de Proteção de Dados Pessoais (LGPD) e outras legislações relacionadas à segurança cibernética.

3.2. O projeto em questão visa minimizar a vulnerabilidade dos sistemas corporativos, redes, estações de trabalho, caixas postais, implementando metodologias de segurança de antivírus corporativo, prevenindo possíveis ataques internos e externos de vírus, spams e spywares e outras ameaças virtuais

ao ambiente tecnológico da Secretaria.

3.3. Além disso, a contratação visa estabelecer práticas de segurança cibernética sólidas, alinhadas com as melhores práticas e padrões do setor. Esse enfoque na segurança cibernética é essencial para mitigar riscos e proteger a integridade dos dados da Secretaria, sendo fundamental para garantir um ambiente seguro e confiável para a manipulação e proteção dos dados pessoais, cumprindo as exigências legais e fortalecendo a postura de segurança da SEAD-PI.

3.4. O projeto em questão está em conformidade e encontra-se alinhado ao Plano Plurianual – PPA (2024-2027), instrumento de planejamento do Governo do Estado, mais especificamente com o Programa 0109 – GESTÃO, INOVAÇÃO E TRANSFORMAÇÃO DIGITAL – Objetivo: Integrar e ampliar a oferta de serviços públicos, garantindo a eficiência, eficácia e efetividade na ação governamental com foco na governança, na transformação digital e na gestão por resultados.

4. NECESSIDADES TECNOLÓGICAS

4.1. A solução de segurança proposta, para proteção de e-mail, endpoint e redes, tem como deverá contribuir para garantir um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas nos meios tecnológicos da SEAD-PI.

4.2. A solução deve suportar as seguintes funcionalidades:

4.3. Reputação de Arquivos: tanto para arquivos locais quanto para acesso web, a solução deve fornecer mecanismos para avaliar a reputação dos arquivos, identificando possíveis ameaças e evitando que arquivos maliciosos sejam abertos ou executados.

4.4. Redução de riscos: a solução deve fornecer acesso imediato à percepção e ao controle de segurança, permitindo uma resposta rápida a incidentes e minimizando os riscos associados a ameaças em potencial.

4.5. Aprendizado de Máquinas (Machine Learning) e Análise Comportamental (Behavioral Analysis): utilizando técnicas de aprendizado de máquinas e análise comportamental, a solução deve ser capaz de identificar comportamentos suspeitos e atividades maliciosas, fornecendo uma camada adicional de proteção contra ameaças desconhecidas.

4.6. Mitigação da Exploração de Memória (Memory Exploit Mitigation): a solução deve incluir mecanismos de mitigação de ataques que explorem vulnerabilidades de memória, protegendo contra técnicas como injeção de código malicioso e estouro de buffer.

4.7. Minimização da complexidade: a solução deve criar uma estrutura de gerenciamento centralizada e integrada, facilitando o gerenciamento de segurança e proporcionando uma defesa unificada. Além disso, deve oferecer visibilidade aos clientes e serviços monitorados, permitindo uma visão abrangente da postura de segurança da SEAD-PI.

4.8. Gerenciamento de patches e scanning de vulnerabilidades: a solução deve possibilitar o gerenciamento centralizado de patches de segurança, permitindo a detecção de vulnerabilidades e a aplicação de correções de forma eficiente e simplificada.

4.9. Minimização do impacto de ameaças: a solução deve permitir respostas automáticas a incidentes, ganhando tempo na mitigação de ameaças e reduzindo o impacto causado por ataques.

4.10. A implementação dessa solução tecnológica deverá atender as necessidades de segurança da SEAD-PI, proporcionando uma proteção abrangente e eficaz contra ameaças cibernéticas, garantindo a integridade e confidencialidade das informações e fortalecendo a postura de segurança da organização.

5. DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC

5.1. REQUISITOS DE CAPACITAÇÃO

5.1.1. A empresa CONTRATADA deverá realizar o repasse de conhecimento aos funcionários da CONTRATANTE que atuarão, diretamente, com a solução de segurança adquirida, contemplando instalação, parametrização, monitoramento, melhores práticas e atuação de incidentes com carga horária mínima de 40 (quarenta) horas ministrado por profissional certificado pelo fabricante.

5.1.2. O treinamento será demando à CONTRATADA pela CONTRATANTE após a efetiva implementação e estruturação da solução de segurança em seu parque tecnológico, quando acordarão cronograma para realização do treinamento.

5.1.3. O treinamento deverá ser realizado na modalidade presencial nas dependências da CONTRATANTE a participantes da equipe técnica a serem definidos pela CONTRATANTE.

5.1.4. Os horários do curso deverão seguir a conveniência do CONTRATANTE, podendo sua realização ocorrer apenas em um dos períodos do dia (manhã ou tarde).

5.1.5. Deverá ser fornecido material didático completo e com conteúdo oficial do fabricante em língua portuguesa. Caso seja utilizado material elaborado exclusivamente pelo fabricante e fique demonstrado que este não é oferecido em língua portuguesa, será aceito o fornecimento em língua inglesa.

5.1.6. O treinamento deve conter parte teórica e prática, incluindo tópicos sobre a instalação, uso, configuração, resolução de problemas da solução, análise de relatórios, respostas a incidentes e outros.

5.1.7. As datas do treinamento devem ser previamente combinadas com o CONTRATANTE.

5.1.8. Todos os custos relativos à realização do treinamento são de exclusiva responsabilidade da CONTRATADA.

5.2. REQUISITOS E FUNCIONALIDADES TÉCNICOS DA SOLUÇÃO

5.2.1. A especificação técnica mínima e obrigatória da solução encontra-se detalhada no **Anexo I** deste estudo.

5.3. REQUISITOS DE MANUTENÇÃO E GARANTIA

5.3.1. A empresa contratada é responsável por fornecer suporte técnico e garantia de atualização da solução pelo período de 24 meses, a contar da data de emissão do Termo de Recebimento. É importante ressaltar que essa garantia não se limita ao término da vigência contratual.

5.3.2. A garantia deve incluir obrigatoriamente:

5.3.3. Atualização das versões dos softwares fornecidos, caso sejam disponibilizadas novas versões.

5.3.4. Atualização dos softwares fornecidos caso haja lançamento de novos softwares que substituam os fornecidos ou se ficar evidente a descontinuidade dos softwares fornecidos, mesmo que não se trate de substituição direta.

5.3.5. Correções dos softwares fornecidos, incluindo a aplicação de patches para corrigir eventuais falhas (bugs) de software que possam prejudicar o ambiente de produção ou vulnerabilidades que comprometam a segurança da solução.

5.3.6. A garantia deverá ser prestada durante todo o período de contrato e aditivos relacionados à atualização das licenças e proteção.

5.3.7. Durante o período de garantia, a empresa contratada compromete-se a substituir, em até 15 dias úteis, os equipamentos que apresentarem, em um período de 60 dias, duas ocorrências de defeitos por inoperância do produto ou 3 ocorrências de deficiência operacional do produto.

5.3.8. As ferramentas e equipamentos necessários à manutenção serão de responsabilidade da contratada.

5.4. **SUPORTE TÉCNICO**

Deverá ser oferecido suporte técnico da Contratada, com a possibilidade de abertura de chamados, das 7h00 às 20h00, em dias úteis, para a resolução de problemas. É importante destacar que os serviços de suporte técnico devem contemplar as manutenções corretivas e evolutivas para a solução contratada e não podem acarretar custos adicionais ao CONTRATANTE, além do que foi previamente acordado.

5.4.1. A empresa contratada deve encaminhar o chamado para o suporte do fabricante sempre que necessário, seja devido à criticidade, impacto ou urgência do problema, ou caso seja necessário o envolvimento direto do fabricante no processo de correção. É imprescindível que seja fornecido acesso ao site do fabricante para acompanhamento dos chamados, acesso à base de conhecimento e aos fóruns relacionados à solução.

5.4.2. Os serviços de suporte técnico abrangem:

- Manutenção preventiva, manutenção corretiva, esclarecimento de dúvidas e reparação de problemas na solução.
- Elaboração de relatórios, estudos e diagnósticos sobre o ambiente.
- Transferência de conhecimento aos técnicos da Contratante referente aos problemas vivenciados e às soluções aplicadas, na forma a ser determinada pelas partes.
- Realização de instalação, atualização e configuração de novas versões dos produtos após a disponibilização das atualizações tecnológicas pelo fabricante.

5.4.3. O suporte técnico deve contemplar o atendimento para sanar dúvidas relacionadas com instalação, configuração e uso do software ou para correção de problemas, em especial na configuração de parâmetros, falhas, erros, defeitos ou vícios identificados no funcionamento da solução.

5.4.4. O suporte técnico deve contemplar, quando for o caso, atendimento a eventual problema de instalação ou configuração de softwares básicos e de infraestrutura de TIC (sistemas operacionais, servidores de banco de dados, servidores de aplicação, etc.) necessários ao funcionamento da solução.

5.4.5. Deve contemplar também a atualização de versões do software aplicativo, as quais incorporam correções de erros ou problemas registrados e melhorias implementadas pela fabricante, num empacotamento estável do sistema. O serviço de atualização de versão tem por finalidade assegurar a devida atualização da solução durante o período de vigência da garantia. Refere-se ao fornecimento de novas versões e releases da solução lançados no período. A cada nova liberação de versão e release, serão disponibilizados em formato digital manuais e demais documentos técnicos, bem como nota informativa das funcionalidades implementadas. Em caso de lançamento de patch de correção, a CONTRATADA deverá comunicar o fato ao CONTRATANTE e indicar a forma de obtenção e os defeitos que serão corrigidos pelo patch. Em ambos os casos, a comunicação deve ser feita no prazo de até 30 dias, a contar do lançamento de nova versão ou solução de correção.

5.4.6. A CONTRATADA será responsável pelos serviços de implantação das novas versões e releases dos produtos por ela fornecidos como partes do objeto, bem como pela aplicação dos patches de correção e pacotes de serviço (service packs) relativos a esses produtos. Para a implantação das novas versões/releases, bem como para a aplicação dos patches, deverá ser aberto chamado de suporte técnico com nível de severidade adequado e a prestação dos serviços deve ser agendada com os responsáveis pela solução na CONTRATANTE;

5.4.7. Deverá ser prestado suporte técnico remoto com atendimento mediante registro de chamados em página de website, em sistema fornecido pela CONTRATADA e/ou pelo fabricante; e também através de contato telefônico. Esse serviço destina-se a esclarecimento de dúvidas e resolução de problemas relacionados à configuração e uso dos componentes da solução CONTRATADA;

5.4.8. As peças substitutas deverão apresentar padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento e devem integrar a garantia da solução;

5.4.9. A CONTRATADA auxiliará o CONTRATANTE na reinstalação das ferramentas, caso seja necessário, ao longo do tempo de garantia da ferramenta;

5.4.10. A CONTRATADA deverá disponibilizar os seguintes canais de acesso ao suporte técnico:

- Portal Web;
- E-mail;
- Central 0800; e/ou
- Telefone fixo.

5.4.11. O atendimento deve ser contínuo, 24 horas por dia, 7 dias por semana, durante todo o ano, incluindo feriados, em língua portuguesa. O início do atendimento e o prazo de solução devem ser determinados de acordo com o nível de severidade exigido para o caso, conforme os índices de criticidade abaixo:

Criticidade	Descrição	Prazo Máximo de Atendimento	Prazo Máximo de Restauração de Serviço	Glosa (por evento) para eventual descumprimento
Severidade 1 (Alta)	Sistema parado ou produto inoperante com impacto nas operações críticas de negócio. Exemplos: Servidor de produção ou outro sistema inicial está inativo. Parte substancial dos dados essenciais corre risco de perda ou corrupção. Operações relacionadas ao negócio	Em até 2 horas deve ter um técnico do fornecedor on-site.	Em até 8 horas	10%

Criticidade	Descrição	Prazo Máximo de Atendimento	Prazo Máximo de Restauração de Serviço	Glosa (por evento) para eventual descumprimento
	foram afetadas, falha que compromete a integridade geral do sistema ou dos dados.	Em até 4 horas deve ter um técnico do fornecedor on-site.	Entrega da Solução pelo fabricante em até 6 dias.	
Severidade 2 (Média/Alta)	Alto impacto no ambiente de produção ou grande restrição de funcionalidade. Exemplo: Ocorreu um problema no qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade a longo prazo possa ser afetada negativamente.	Em até 4 horas deve ter um técnico do fornecedor on-site.	Em até 4 horas deve ter um técnico do fornecedor on-site.	7,50%
		Em até 2 horas um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone ou retorno de chamada. Gerente técnico do fabricante deve estar disponível 24x7 e ser automaticamente notificado na abertura do caso.	Em até 16 horas	
			Entrega da Solução pelo fabricante em até 10 dias.	
Severidade 3	O defeito não gera impacto ao negócio. Exemplo: Ocorreu um erro que causou impacto negativo limitado na operações.	Um técnico do fornecedor on-site ou atendimento remoto.	Em até 24 horas.	5%
		Em até 6 horas um Engenheiro de Suporte do fabricante entra em contato.	Entrega da Solução pelo fabricante em até 15 dias ou na próxima atualização do Software.	
Severidade 4 (Baixa)	O problema é pequeno, ou de documentação. Exemplos: O problema não afetou as operações da contratante negativamente; Encaminhamento de solicitações e ou sugestões para novos recursos ou aprimoramento do software licenciado.	Em até 12 horas um técnico do fornecedor entra em contato.	Em até 12 horas um técnico do fornecedor entra em contato.	2%
		No mesmo dia ou no próximo dia útil comercial.	No mesmo dia ou no próximo dia útil comercial.	

5.4.12. Para cada chamado de suporte categorizado como grau de severidade 1, o recurso previsto na tabela acima deverá ser notificado e iniciará o auxílio na condução do processo internamente junto ao fabricante. É importante destacar que todos os prazos para atendimento da garantia começarão a ser contados a partir da abertura do chamado, independentemente de ter sido feito via telefone, e-mail, site da contratada ou do fabricante. Além disso, o período de suporte deve estar diretamente atrelado ao período de garantia da solução.

5.4.13. Dentro do prazo máximo de atendimento, cabe ao fornecedor dar início, junto ao contratante, às providências que serão adotadas para a solução do chamado. Considera-se plenamente solucionado o problema quando os sistemas/serviços forem restabelecidos sem restrições, ou seja, quando não se tratar de uma solução paliativa.

5.4.14. Para os chamados de severidades 1 e 2, os serviços de atendimento de garantia não podem ser interrompidos até o completo restabelecimento de todas as funções do sistema paralisado, mesmo que isso exija períodos noturnos e dias não úteis (sábados, domingos e feriados). Além disso, os chamados de garantia de severidades 1 e 2 devem contar com suporte in loco da contratada para agilizar o restabelecimento do serviço.

5.4.15. O fornecedor emitirá um relatório, sempre que solicitado pelo contratante, em formato eletrônico, preferencialmente em arquivo texto, contendo informações analíticas e sintéticas dos chamados da garantia abertos e fechados no período. Esse relatório deve incluir:

I - Quantidade de ocorrências (chamados) registradas no período.

II - Número do chamado registrado e nível de severidade, incluindo reaberturas. Data e hora de abertura.

III - Data e hora de início e conclusão do atendimento.

IV - Identificação do técnico do contratante que registrou o chamado.

V - Identificação do técnico do contratante que atendeu o chamado da garantia. Descrição do problema.

VI - Descrição da solução.

VII - Informações sobre eventuais escalonamentos.

VIII - Resumo da lista de chamados concluídos fora do prazo de solução estabelecido.

IX - Total de chamados no mês e o total acumulado até a apresentação do relatório.

5.4.16. Deverá ser emitido um relatório de histórico e revisão de casos, fornecido pelo gerente técnico do fabricante, sob os chamados abertos ou de responsabilidade do fabricante.

5.4.17. Deverá ser emitido um relatório de histórico e revisão de casos, fornecido pelo gerente técnico do fabricante, sob os chamados abertos ou de responsabilidade do fabricante.

5.4.18. Não se encaixam nos prazos descritos nos itens referentes aos níveis de criticidade, problemas cuja solução dependa de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução.

5.4.19. Para esses problemas, o fornecedor deverá, nos prazos estabelecidos nos níveis de criticidade, restabelecer o ambiente, através de uma solução de contorno e informar ao contratante, em um prazo máximo de 24 (vinte e quatro) horas, quando a solução definitiva será disponibilizada para o contratante.

5.4.20. Esta solução definitiva de que trata o subitem anterior deverá ser disponibilizada no prazo máximo de 60 (sessenta) dias úteis, no caso da necessidade de criação de um patch/fix.

5.5. **REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS**

5.5.1. A Contratada deve aderir aos padrões estabelecidos pelo Modelo de Acessibilidade em Governo Eletrônico (e-MAG), conforme a Portaria Normativa SLTI nº 03, de 7 de maio de 2007. Essa aderência é necessária quando houver a necessidade de tornar o aplicativo acessível para solicitações de suporte técnico, visando garantir a inclusão e acessibilidade para todos os usuários.

5.5.2. Os serviços prestados pela Contratada devem sempre considerar o uso racional de recursos e equipamentos, com o objetivo de evitar o desperdício de insumos e materiais, bem como a geração excessiva de resíduos. Essa prática está alinhada com as diretrizes de responsabilidade ambiental adotadas pela Contratante.

5.5.3. A Contratada é responsável por fornecer orientações aos seus funcionários sobre a importância da racionalização de recursos no desempenho de suas atribuições, assim como sobre as diretrizes de responsabilidade ambiental adotadas pela Contratante. Essas orientações devem destacar a importância de reduzir o consumo de recursos, reutilizar materiais sempre que possível e realizar descarte adequado dos resíduos.

5.5.4. Além disso, a Contratada deve autorizar a participação de seus funcionários em eventos de capacitação e sensibilização promovidos pela Contratante, quando necessário. Esses eventos têm como objetivo fornecer conhecimentos e práticas relacionadas à racionalização de recursos e responsabilidade ambiental, visando aprimorar a conscientização e o desempenho sustentável da equipe da Contratada.

5.6. **REQUISITOS TEMPORAIS**

5.6.1. As diretrizes relacionadas aos requisitos a seguir deverão ser considerados no processo de atendimento, entrega e instalação de equipamentos e serviços:

Prazo de início de atendimento para suporte técnico e manutenção pela garantia:

O início do atendimento deve seguir o que está especificado no acordo de nível de serviço presente no Termo de Referência.

Prazo de entrega e instalação:

O prazo de entrega e instalação deve estar de acordo com o que foi especificado no Termo de Referência. Caso não haja uma definição específica, o prazo padrão será considerado conforme a ordem de serviço.

Local de entrega dos equipamentos e licenças de software:

Os equipamentos e licenças de software devem ser entregues conforme disposto no Termo de Referência.

Horário de entrega dos equipamentos/serviços:

A entrega dos equipamentos/serviços deve ocorrer entre as 08:00 e 15:00. É possível agendar uma data e hora específica previamente com a CONTRATANTE.

Verificação da conformidade dos materiais entregues:

É responsabilidade da CONTRATANTE rejeitar, total ou parcialmente, os materiais entregues que não estejam de acordo com o objeto definido no Termo de Referência.

Recebimento dos produtos:

O recebimento dos produtos será feito pela equipe designada pela CONTRATANTE. Esse recebimento ocorrerá de forma provisória no momento da entrega dos equipamentos e de forma definitiva após a instalação, configuração e teste da solução.

5.7. **REQUISITOS DE SEGURANÇA E PRIVACIDADE**

5.7.1. A CONTRATADA deve seguir os regulamentos, normas e instruções de segurança da informação e comunicações adotados pela CONTRATANTE. Isso inclui a Política de Segurança da Informação e Comunicações e suas Normas Complementares durante a execução dos serviços nas instalações da Secretaria.

Garantia da disponibilidade, integridade, confidencialidade e sigilo das informações:

A empresa CONTRATADA deve assegurar a disponibilidade, integridade, confidencialidade e sigilo dos documentos e informações relacionados ao contrato e aos serviços prestados. Qualquer pessoa que cause perdas e danos à CONTRATANTE ou a terceiros poderá ser responsabilizada legalmente.

Devolução de informações confidenciais:

Toda informação confidencial gerada e/ou manipulada em decorrência do contrato, seja ela armazenada em meio físico, magnético ou eletrônico, deve ser devolvida nas seguintes situações:

a) término ou rompimento do contrato; ou

b) solicitação da CONTRATANTE. A formalização entre as partes é necessária nesses casos.

Utilização de ferramentas de proteção e segurança de informações:

É imprescindível o uso de ferramentas de proteção e segurança de informações para evitar acesso não autorizado aos sistemas e softwares. Isso se aplica tanto aos sistemas sob responsabilidade direta da CONTRATADA quanto aos disponibilizados à CONTRATANTE, mesmo que por meio de link.

Realização de alterações para sanar problemas de segurança ou vulnerabilidade:

Quando formalmente solicitado pela CONTRATANTE, a CONTRATADA deve priorizar e realizar alterações para solucionar possíveis problemas de segurança ou vulnerabilidade nos sistemas ou softwares utilizados para a execução do serviço contratado.

Comunicação de atualizações ou mudanças na configuração dos serviços:

A CONTRATADA deve informar formalmente e de forma tempestiva ao CONTRATANTE sobre quaisquer necessidades de atualização ou mudança na configuração dos serviços prestados.

Prestação de esclarecimentos e informações:

É responsabilidade da CONTRATADA prestar os esclarecimentos necessários à CONTRATANTE, bem como fornecer informações sobre a natureza e o andamento dos serviços executados ou em execução.

Garantia da integridade e disponibilidade dos documentos e informações:

A empresa CONTRATADA deve garantir a integridade e disponibilidade dos documentos e informações que estão sob sua guarda em função do contrato. Caso ocorram perdas ou danos, a CONTRATADA será responsabilizada.

Confidencialidade das informações:

A CONTRATADA não pode divulgar, mesmo que em caráter estatístico, quaisquer informações originadas na CONTRATANTE sem prévia autorização.

Controle de acesso e identificação dos profissionais:

O acesso às instalações da CONTRATADA onde os serviços serão realizados deve ser controlado e permitido apenas para pessoas autorizadas. Os profissionais da CONTRATADA devem estar devidamente identificados por crachás durante o trabalho. Qualquer profissional considerado inconveniente à boa ordem ou que viole as normas disciplinares da CONTRATANTE deve ser substituído imediatamente.

Conhecimento e observância das normas disciplinares da CONTRATANTE:

A CONTRATADA deve garantir que seus profissionais tenham conhecimento das normas disciplinares do CONTRATANTE e exijam sua fiel observância, especialmente em relação à utilização e segurança das instalações.

A CONTRATADA deve manter sigilo absoluto sobre todas as informações provenientes dos serviços realizados, documentos elaborados e informações obtidas dentro do ambiente da CONTRATANTE.

5.8. REQUISITOS LEGAIS

5.8.1. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021 (Lei de Licitações e Contratos Administrativos), à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis;

6. ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS

6.1. A Secretaria de Estado de Administração e Previdência realizou um levantamento para determinar a quantidade de bens e serviços necessários para atender às demandas dos usuários. Atualmente, há aproximadamente 2.000 usuários ativos na rede, 1.200 estações de trabalho, além de caixas postais e outros recursos.

6.2. Os números apresentados são baseados na infraestrutura computacional atual, considerando o número de estações de trabalho, notebooks e outros recursos existentes na instituição. Contudo, é imprescindível considerar o crescimento contínuo da infraestrutura computacional e as novas demandas decorrentes das tecnologias emergentes. Ademais, o aumento previsto no número de dispositivos, resultado de futuros processos de aquisição, pode acarretar alterações significativas nos quantitativos mencionados, tornando difícil uma precisão absoluta na definição do quantitativo necessário.

6.3. Considerando as informações apresentadas e a participação da Secretaria de Estado da Saúde do Piauí (SESAPI), Secretaria de Estado da Educação do Piauí (SEDUC) neste projeto, a equipe de planejamento da contratação recomenda a adoção do Registro de Preços. Essa escolha é respaldada pelos princípios da viabilidade técnica, respeito à economicidade e planejamento estratégico. O Registro de Preços se destaca como a opção mais

apropriada, proporcionando flexibilidade para ajustar as quantidades conforme as demandas reais de cada unidade, especialmente diante das dinâmicas variáveis do ambiente.

6.4. Diante da recomendação acima, a SEAD-PI formalizou o envio de ofícios às secretarias coparticipantes para a definição dos quantitativos estimados, alinhados com as demandas específicas de cada entidade. Abaixo, apresentamos a consolidação preliminar desses quantitativos, baseada nas informações disponíveis até o momento:

Item	Descrição do Item	Unidade de Medida	Quantidade			Total
SESAPI	SEDUC	SEAD-PI				
1	Solução de proteção de Endpoints com abordagem proativa para resposta eficaz a incidentes	Por Endpoint	2500	10000	1200	6800
2	Solução de proteção de Servidores com abordagem proativa para resposta eficaz a incidentes	Por Servidor	100	375	20	544
3	Solução de segurança avançada para mitigação de ameaças na rede	Por Throughput de dados	3	4	2	6
4	Solução de prevenção de intrusão de próxima geração (NGIPS)	Por Throughput de dados	3	5	2	1
5	Solução de Gerenciamento de Vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança.	Por dispositivos, assets, aplicações web, contêiner	100	375	1220	20
6	Solução de Gerenciamento de Vulnerabilidades e Visibilidade de Ataques em tempo real para estrutura de Diretório de Usuários, com análise contínua e adaptável de riscos e confiança.	Por de usuários ativos no Active Directory	0	10000	1200	4300
7	Serviço de suporte pro ativo, corretivo e para resposta a incidentes	Por Solução	5	9	9	10
8	Serviço de implantação	Por Solução	5	9	9	10
9	Serviço de capacitação e repasse de conhecimento	40 Horas	5	8	5	4
10	Serviço de monitoramento do ambiente presencial	Por Posto	0	1	1	3

6.5. É importante ressaltar que esses números estão sujeitos a alterações e ajustes, conforme a evolução da infraestrutura e das demandas tecnológicas. Portanto, a criação de Registro de Preço permitirá uma gestão mais eficiente e adaptável da quantidade de bens e serviços necessários para atender às demandas da Secretaria de Estado de Administração e Previdência.

7. LEVANTAMENTO DE SOLUÇÕES

7.6. Identificação das Possíveis Soluções

ID	Descrição do Solução/Cenário
1	Registro de Preços para contratação de empresa para fornecimento, sob demanda, de solução de segurança para proteção de e-mail, Endpoint e proteção contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, para atender às necessidades dos órgãos e entes da Administração Pública, pelo período de 24 meses.
2	Adoção de solução baseada em software livre.

7.7. Identificação das Possíveis Soluções

7.7.1. Solução/Cenário 1

7.7.1.1. O Cenário 1 propõe a utilização do Registro de Preços para contratação sob demanda de uma empresa que forneça uma solução de segurança abrangente para proteção de e-mail, endpoints e defesa contra ataques avançados. Essa contratação engloba serviços de instalação, configuração, transferência de conhecimento, suporte técnico e garantia, com o intuito de atender às necessidades da Secretaria de Estado de Administração e Previdência ao longo de um período de 24 meses.

7.7.1.2. Essa solução de Tecnologia da Informação e Comunicação (TIC) tem por finalidade proteger as estações de trabalho contra ameaças comuns da internet, como vírus, worms, ransomware, keyloggers, backdoors, rootkits, trojans e spyware. Além disso, a solução inclui funcionalidades avançadas de bloqueio de dispositivos para reforçar a segurança dos sistemas, assegurando a integridade, autenticidade e disponibilidade das informações, essenciais para o pleno funcionamento das atividades da Secretaria.

7.7.1.3. Esta solução também realiza o monitoramento do comportamento das estações de usuários e caixas de e-mail, com o objetivo de detectar, bloquear, investigar e responder a incidentes de segurança da informação que possam surgir na rede da Secretaria.

7.7.1.4. Além das licenças de software, a solução compreende a instalação e configuração da ferramenta, um módulo dedicado à investigação, correlação e resposta a incidentes em endpoints, servidores e e-mails, bem como a disponibilização de conhecimento prático

(hands-on), suporte técnico corretivo e preventivo, juntamente com a garantia do fabricante. Esses serviços estão projetados para atender às necessidades da Secretaria ao longo de um período de 24 meses.

7.7.1.5. Diante dessas considerações e da ausência de justificativas embasadas que recomendem a não adoção deste cenário, a equipe de planejamento entende que essa é a opção mais adequada para atender à atual necessidade da Secretaria.

7.7.2. **Solução/Cenário 2**

7.7.2.1. A opção identificada como Solução 2 se concentra na implementação de software de código aberto, caracterizado por sua adesão aos princípios da liberdade e da comunidade de usuários. Em termos simples, isso significa que os usuários têm a liberdade de executar, copiar, distribuir, estudar, modificar e aprimorar o software.

7.7.2.2. Embora essa abordagem possa ser vista de maneira positiva, é importante considerar que ela traz consigo um desafio significativo em termos de segurança. Isso ocorre porque as personalizações são realizadas sem as devidas considerações em relação à padronização, escalabilidade e consistência, o que pode tornar o sistema vulnerável.

7.7.2.3. Além disso, a atual necessidade da SEAD-PI envolve a obtenção de suporte técnico para a solução ao longo de um período de 24 meses. O software de código aberto não oferece suporte ou garantias, deixando os dados da SEAD-PI dependentes de comunidades de desenvolvedores, sem acordos de nível de serviço (SLA) ou qualquer forma de garantia.

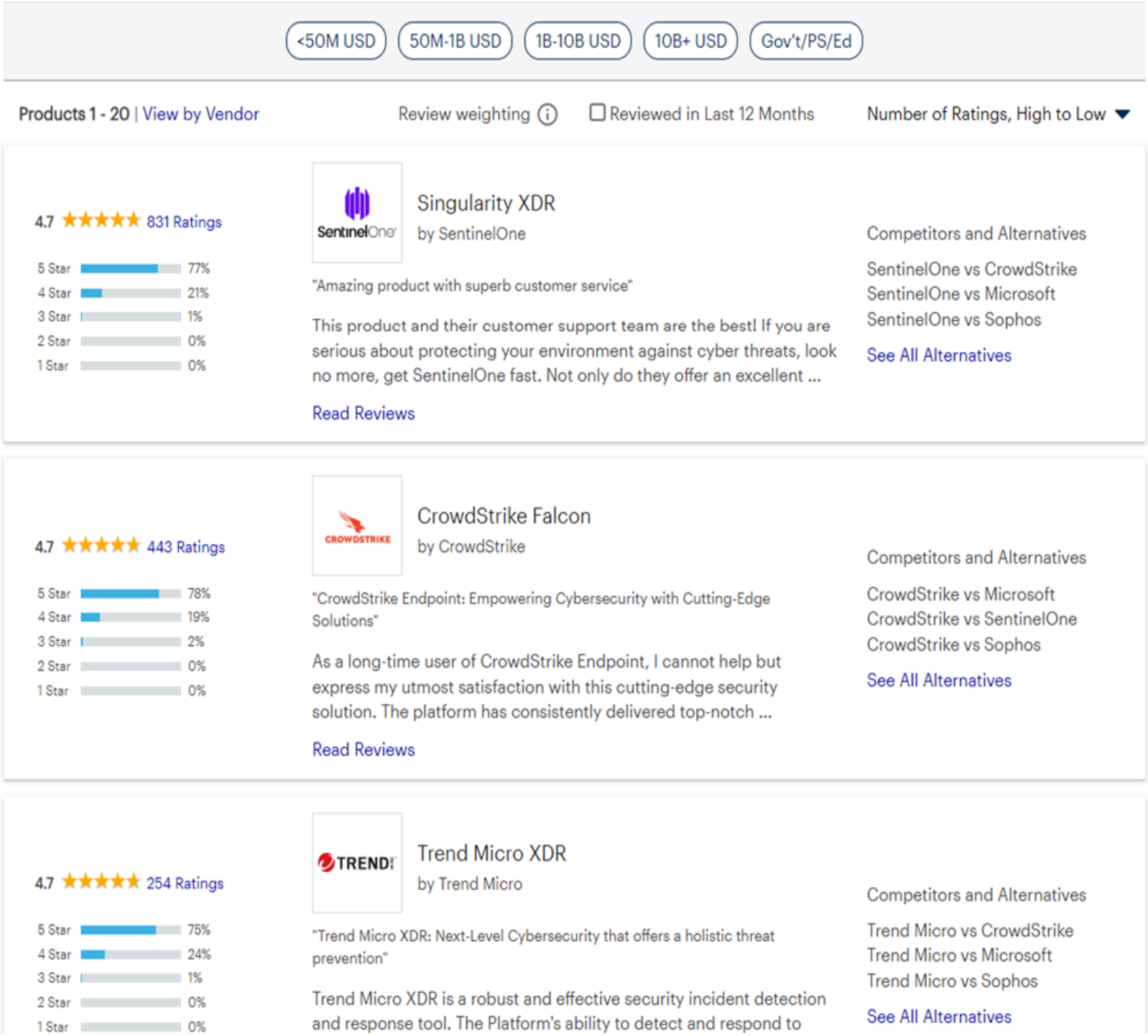
7.7.2.4. Com base nessas razões e na ausência de justificativas objetivas para a adoção desta solução, a equipe de planejamento da contratação não a recomenda.

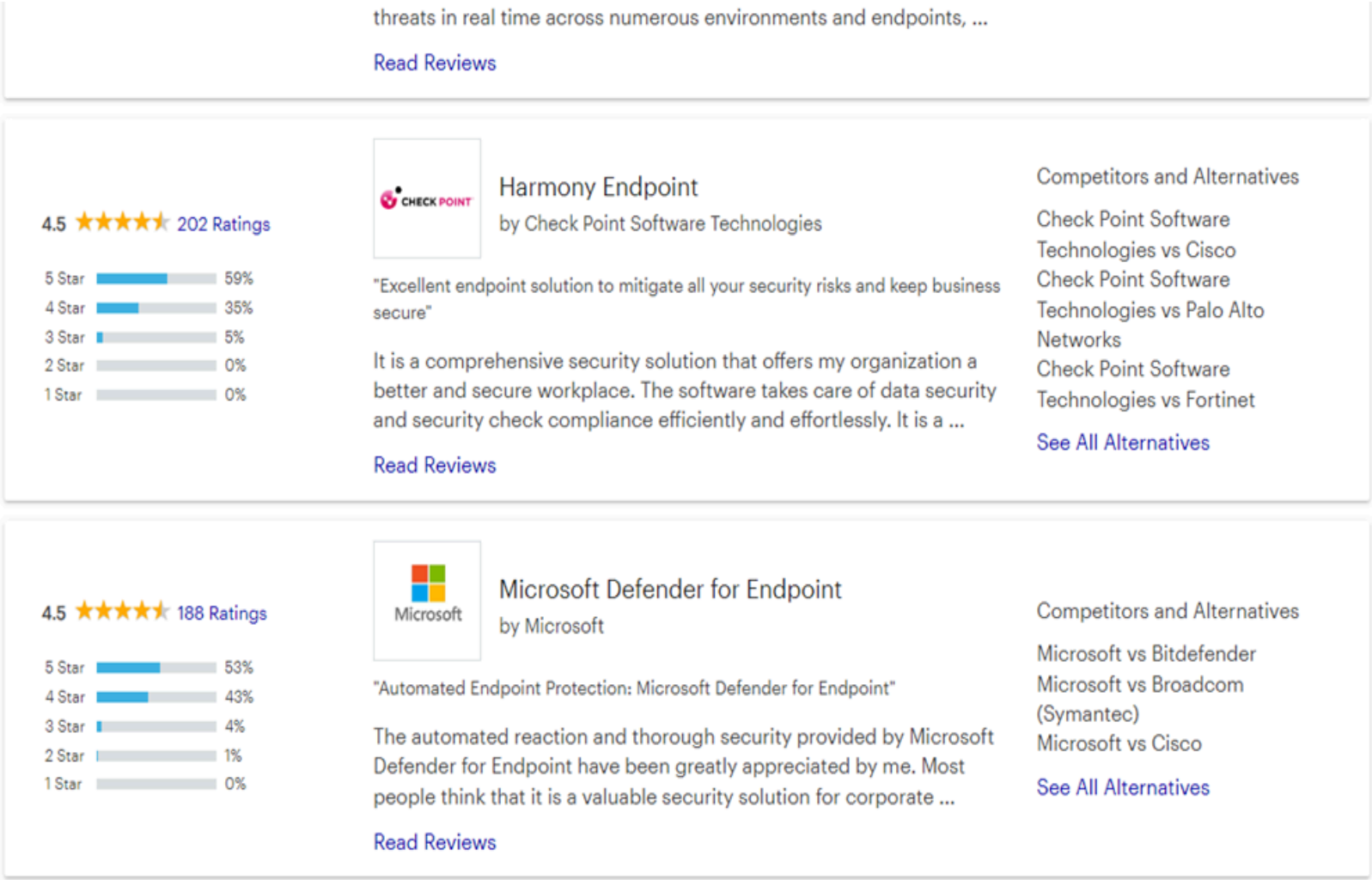
7.8. SOLUÇÕES DISPONÍVEIS NO MERCADO

7.8.1. A proteção física e lógica da informação deve ser provida por ferramentas especializadas, seguras, consolidadas e, acima de tudo, que preservem a confidencialidade, a integridade e a disponibilidade da informação.

7.8.2. Em observância ao disposto na Instrução Normativa SGD/ME IN SGD /ME nº 94/2022, apresenta-se a seguir a avaliação de soluções e a capacidade de cada uma delas para atender aos requisitos de proteção de e-mail, endpoints e defesa contra ataques avançados.

7.8.3. As opções de soluções corporativas para solução de segurança para proteção de e-mail, Endpoint e proteção contra ataques avançados disponíveis no mercado são vastas e apresentam diversas versões. Para auxiliar na análise, segue abaixo uma lista dos 5 principais fabricantes de soluções, classificados pelo Gartner de acordo com o número de avaliações, do mais alto ao mais baixo.


<50M USD
50M-1B USD
1B-10B USD
10B+ USD
Gov't/PS/Ed
Products 1 - 20 | View by Vendor
Review weighting
Reviewed in Last 12 Months
Number of Ratings, High to Low
4.7 831 Ratings
5 Star 77%
4 Star 21%
3 Star 1%
2 Star 0%
1 Star 0%
Singularity XDR
by SentinelOne
"Amazing product with superb customer service"
This product and their customer support team are the best! If you are serious about protecting your environment against cyber threats, look no more, get SentinelOne fast. Not only do they offer an excellent ...
Read Reviews
Competitors and Alternatives
SentinelOne vs CrowdStrike
SentinelOne vs Microsoft
SentinelOne vs Sophos
See All Alternatives
4.7 443 Ratings
5 Star 78%
4 Star 19%
3 Star 2%
2 Star 0%
1 Star 0%
CrowdStrike Falcon
by CrowdStrike
"CrowdStrike Endpoint: Empowering Cybersecurity with Cutting-Edge Solutions"
As a long-time user of CrowdStrike Endpoint, I cannot help but express my utmost satisfaction with this cutting-edge security solution. The platform has consistently delivered top-notch ...
Read Reviews
Competitors and Alternatives
CrowdStrike vs Microsoft
CrowdStrike vs SentinelOne
CrowdStrike vs Sophos
See All Alternatives
4.7 254 Ratings
5 Star 75%
4 Star 24%
3 Star 1%
2 Star 0%
1 Star 0%
Trend Micro XDR
by Trend Micro
"Trend Micro XDR: Next-Level Cybersecurity that offers a holistic threat prevention"
Trend Micro XDR is a robust and effective security incident detection and response tool. The Platform's ability to detect and respond to
Competitors and Alternatives
Trend Micro vs CrowdStrike
Trend Micro vs Microsoft
Trend Micro vs Sophos
See All Alternatives



7.8.4. As soluções ranqueadas fornecem os recursos principais a seguir:

SOLUÇÃO	**PRINCIPAIS RECUROS**
Singularity XDR (SentinelOne)	• Automatização detecção e resposta de Endpoint; • Proteção de carga de trabalho; • Modelo de prevenção com tecnologia de IA;

SOLUÇÃO	**PRINCIPAIS RECUROS**
	● Detecção e resposta proativas em tempo real.
CrowdStrike Falcon (CrowdStrike)	● Antivírus de última geração (NGAV); ● Detecção e resposta de endpoint; ● Investigação gerenciada de ameaças; ● Inteligência de ciberameaça.
Trend Micro XDR (Trend Micro)	● Correlação avançada de ameaças; ● Investigação e resposta rápidas a ameaças; ● Detecção precoce e precisa de ameaças; ● Detecção e resposta em Endpoints.
Harmony Endpoint (Check Point Software Technologies)	● Proteção completa de endpoint; ● Anti-Ransomware;

SOLUÇÃO	**PRINCIPAIS RECUROS**
	• Proteções de ataque de malware e file-less; • Prevenção de roubo de credenciais.
Microsoft Defender for Endpoint (Microsoft)	• Gerenciamento de vulnerabilidades com base em risco; • Proteção habilitada para a nuvem e baseada em comportamento; • EDR (Detecção e Resposta de Ponto de Extremidade); • Investigação e correção automática.

7.8.5. Como se pode observar, há diversas opções disponíveis no mercado com recursos avançados para proteção e segurança cibernética. Cada uma das soluções apresentadas possui características específicas que visam atender às necessidades das organizações em termos de detecção, resposta e prevenção de ameaças. Essas soluções são desenvolvidas por fabricantes renomados e reconhecidos pelo Gartner, o que confere uma qualidade e confiabilidade adicionais.

8. ANÁLISE COMPARATIVA DAS SOLUÇÕES

8.9. Disponibilidade de solução similar em outro órgão ou entidade da Administração Pública

8.9.1. Avaliando as soluções adquiridas em contratações recentes pela Administração Pública, que servem como referência, constatamos que estas apresentam configurações aproximadas ou similares às que a SEAD-PI pretende adquirir. Dessa forma, é possível caracterizar a contratação como uma aquisição de natureza comum, uma vez que as configurações padronizadas são amplamente disponíveis no mercado e são frequentemente utilizadas em contratos da Administração Pública.

8.9.2. A análise a seguir apresenta a conformidade das soluções com as políticas, modelos e padrões governamentais, tais como o ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, sempre que aplicáveis:

Requisito	ID Entidade	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	1	X		
	2		X	
A Solução está disponível no Portal do Software Público Brasileiro?	1		X	
	2	X		
A capacidade e alternativas do mercado, inclusive existência de software livre ou software público?	1		X	
	2	X		
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	1	X		

Requisito	ID Entidade	Sim	Não	Não se Aplica
	2		X	
A Solução é aderente às regulamentações da ICP- Brasil? (Quando houver necessidade de certificação digital)	1			X
	2			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do – e-ARQ Brasil?	1	X		
	2		X	
A Solução é aderente às necessidades técnicas do órgão?	1	X		
	2		X	
A análise de projetos similares foi utilizada para realização do orçamento estimado?	1	X		
	2		X	

9. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

9.10. A Solução Identificada com id 2 envolve a utilização de software de código aberto. Entretanto, diante da ausência de suporte técnico especializado, a complexidade de integração de múltiplos produtos para atender de forma aproximada às necessidades e a falta de garantias, torna-se evidente que esta abordagem não é apropriada para atender às exigências da Secretaria.

10. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

10.11. Cálculo dos Custos Totais de Propriedade (TCO)

10.11.1. A equipe de Planejamento da Contratação conduziu uma pesquisa de preços, levando em consideração os diversos componentes e serviços necessários para implementar e manter a Solução 1. Esses componentes incluem licenças de software, hardware, custos de instalação, suporte técnico, atualizações e manutenção contínua.

10.11.2. Com base nos dados coletados durante a pesquisa de preços, a equipe calculou o TCO da Solução 1 ao longo de um período de 24 meses. Esse cálculo leva em consideração não apenas os custos iniciais de aquisição e implementação, mas também os custos contínuos ao longo do tempo, como renovações de licença, atualizações de software e suporte técnico.

10.11.3. Os resultados do cálculo do TCO fornecem uma visão abrangente dos custos totais associados à implementação e manutenção da Solução 1 ao longo de três anos. Essas informações são essenciais para a tomada de decisões informadas, permitindo que a SEAD-PI avalie a viabilidade financeira da solução e compare-a com outras opções disponíveis no mercado.

10.11.4. É importante ressaltar que o TCO não se limita apenas aos custos financeiros, mas também considera a eficácia e o impacto da solução na segurança e proteção dos sistemas e dados da SEAD-PI. Portanto, a equipe de Planejamento da Contratação também levou em consideração aspectos como a qualidade da solução, recursos de suporte e a reputação do fornecedor no mercado.

Item	Descrição da solução	Estimativa de TCO ao longo dos anos - SEAD	
Ano 1	Ano 2	Total	

Item	Descrição da solução	Estimativa de TCO ao longo dos anos - SEAD		
1	Registro de Preços para contratação de empresa para fornecimento, sob demanda, de solução de segurança para proteção de e-mail, Endpoint e proteção contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, para atender às necessidades dos órgãos e entes da Administração Pública, pelo período de 24 meses.	R$ 11.528.732,70	R$ 4.611.493,08	R$ 6.917.239,62

11. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

11.12. Bens e serviços que compõem a solução

11.12.1. A solução de segurança a ser contratada abrange proteção de e-mail, Endpoint e proteção contra ataques avançados para usuário final, com todos os serviços necessários para uma implementação completa e eficaz. Essa solução deverá atender às necessidades específicas da Secretaria de Estado de Administração e Previdência durante um período de 24 meses. Os componentes que compõem essa solução são os seguintes:

Item	Descrição do Item	Unidade de Medida	Quantidade
1	Solução de proteção de Endpoints com abordagem proativa para resposta eficaz a incidentes	Por Endpoint	6800
2	Solução de proteção de Servidores com abordagem proativa para resposta eficaz a incidentes	Por Servidor	544
3	Solução de segurança avançada para mitigação de ameaças na rede	Por Throughput de dados	136
4	Solução de prevenção de intrusão de próxima geração (NGIPS)	Por Throughput de dados	1
5	Solução de Gerenciamento de Vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança.	Por dispositivos, assets, aplicações web, contêiner	20
6	Solução de Gerenciamento de Vulnerabilidades e Visibilidade de Ataques em tempo real para estrutura de Diretório de Usuários, com análise	Por de usuários ativos no Active Directory	4300

Item	Descrição do Item	Unidade de Medida	Quantidade
	contínua e adaptável de riscos e confiança.		
7	Serviço de suporte pro ativo, corretivo e para resposta a incidentes	Por Solução	10
8	Serviço de implantação	Por Solução	10
9	Serviço de capacitação e repasse de conhecimento	40 Horas	4
10	Serviço de monitoramento do ambiente presencial	Por Posto	3

11.13. **Descrição dos itens que compõem a solução**

11.13.1. **Solução de proteção de Endpoints com abordagem proativa para resposta eficaz a incidentes (Item 1)**

11.13.1.1. Visa oferecer uma camada de defesa endpoints da rede, ajudando a prevenir, detectar e responder a ataques de malware, ransomware, vírus e outras ameaças. As proteções para endpoint geralmente incluem firewalls, antivírus, antimalware, detecção de intrusão, controle de aplicativos, gerenciamento de patches e outras ferramentas de segurança. Elas são essenciais para garantir a segurança dos dispositivos e dos dados armazenados neles, especialmente em ambientes corporativos, onde a proteção dos endpoints é crucial para a segurança global da rede.

11.13.2. **Solução de proteção de Servidores com abordagem proativa para resposta eficaz a incidentes (Item 2)**

11.13.2.1. A proteção para servidores em um ambiente corporativo é de extrema importância porque os servidores são peças fundamentais da infraestrutura de tecnologia da informação de uma empresa. Eles armazenam e processam dados críticos e sensíveis, além de hospedar aplicativos e serviços essenciais para o funcionamento do negócio.

11.13.3. **Solução de segurança avançada para mitigação de ameaças na rede (Item 3)**

11.13.3.1. Solução de segurança avançada para mitigação de ameaças na rede é uma ferramenta de segurança cibernética que oferece uma série de benefícios para redes empresariais. Uma de suas principais vantagens é a detecção avançada de ameaças, sendo capaz de identificar e analisar ameaças sofisticadas que muitas vezes conseguem passar despercebidas por soluções de segurança convencionais proporciona uma visibilidade detalhada da rede, permitindo uma análise minuciosa do tráfego e das atividades em curso. Essa análise detalhada ajuda na identificação de comportamentos suspeitos ou anomalias que podem indicar potenciais ameaças à segurança da rede.

11.13.4. **Solução de prevenção de intrusão de próxima geração (NGIPS) - (Item 4)**

11.13.4.1. Um Sistema de Prevenção de Intrusões de Próxima Geração (NGIPS) oferece uma série de vantagens cruciais para a segurança cibernética de uma organização. Em primeiro lugar, ele é capaz de fornecer uma camada avançada de defesa contra ameaças cibernéticas, identificando e bloqueando ataques em tempo real. Essa capacidade de detecção e resposta rápida a ameaças permite proteger a rede contra malware, ataques de negação de serviço (DDoS), exploração de vulnerabilidades e outras formas de intrusões maliciosas. Além disso, o NGIPS proporciona visibilidade aprofundada da atividade da rede, permitindo uma análise detalhada do tráfego em tempo real. Essa análise contínua e

em profundidade ajuda na identificação precoce de atividades suspeitas ou anomalias que possam indicar um possível ataque, permitindo uma resposta rápida e eficaz.

11.13.5. **Solução de Gerenciamento de Vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança (Item 5)**

11.13.5.1. A solução de Gerenciamento de Vulnerabilidades para Endpoints baseada em análise contínua e adaptável ofereceria um conjunto de ferramentas para identificar, avaliar e mitigar vulnerabilidades em dispositivos finais, como computadores e dispositivos móveis. Essa solução realizaria uma análise contínua do ambiente dos endpoints, identificando e classificando riscos em tempo real, ela incluiria serviços completos, desde a instalação e implementação dos softwares necessários até a garantia técnica e transferência de conhecimento para a equipe de segurança da organização. Isso garantiria não apenas a correta implementação da solução, mas também o suporte contínuo para o gerenciamento eficaz das vulnerabilidades nos endpoints.

11.13.6. **Solução de Gerenciamento de Vulnerabilidades e Visibilidade de Ataques em tempo real para estrutura de Diretório de Usuários, com análise contínua e adaptável de riscos e confiança (Item 6)**

11.13.6.1. Essa solução proporcionaria uma visão abrangente e contínua das vulnerabilidades existentes, fornecendo insights em tempo real sobre possíveis ameaças e ataques direcionados aos sistemas relacionados aos diretórios de usuários. Isso incluiria análises adaptáveis e em tempo real, permitindo identificar e responder rapidamente a possíveis riscos e ameaças emergentes. Além disso, a solução ofereceria serviços completos, desde a instalação e implantação dos softwares necessários até a garantia técnica e a transferência de conhecimento. Isso significa que a equipe responsável pela segurança cibernética receberia suporte completo durante todo o processo, desde a configuração inicial até o uso contínuo da solução.

11.13.7. **Serviço de suporte pro ativo, corretivo e para resposta a incidentes (Item 7)**

11.13.7.1. O serviço abrange suporte proativo, corretivo e resposta a incidentes, visando prevenir problemas, corrigir falhas e reagir rapidamente a eventos adversos para manter a estabilidade e segurança dos sistemas.

11.13.8. **Serviço de implantação (Item 8)**

11.13.8.1. Oferece suporte especializado para implementar soluções de segurança digital em ambientes corporativos. Ele inclui desde a configuração inicial até a integração completa das ferramentas de segurança, garantindo uma instalação eficiente e funcional.

11.13.9. **Serviço de capacitação e repasse de conhecimento (Item 9)**

11.13.9.1. Esse serviço visa fornecer treinamento e transferência de conhecimento para os clientes. Ele oferece capacitação especializada, permitindo que os usuários adquiram habilidades e compreensão sobre o uso eficaz das soluções ou tecnologias implementadas, capacitando-os a gerenciar, operar e manter os sistemas.

11.13.10. **Serviço de monitoramento do ambiente presencial (Item 10)**

11.13.10.1. Esse serviço consiste na vigilância contínua e física do ambiente local de uma empresa ou espaço específico. Ele envolve a supervisão ativa por meio de pessoal designado para garantir a segurança, monitorar atividades e identificar possíveis ameaças ou irregularidades no local físico da organização.

11.14. A escolha dessa solução específica foi baseada nas necessidades e requisitos específicos da Secretaria, levando em consideração fatores como eficácia, integração e suporte técnico.

11.15. Com a implementação dessa solução de segurança abrangente, a Secretaria de Estado de Administração e Previdência poderá fortalecer sua postura de segurança cibernética, protegendo de forma eficaz seus sistemas, dados e infraestrutura de TIC durante todo o período contratual.

11.16. Registre-se que a solução escolhida, resultado deste Estudo Técnico Preliminar, não inclui itens presentes nos Catálogos de Soluções de TIC com Condições Padronizadas publicados pelo Órgão Central do SISP.

12. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

12.17. O custo estimado total da contratação é de R$ 11.528.732,70 (onze milhões quinhentos e vinte e oito mil setecentos e trinta e dois reais e setenta centavos) conforme custos unitários apostos na tabela abaixo:

Item	Descrição do Item	Unidade de Medida	Quantidade	Valor Unitário	Valor Total
1	Solução de proteção de Endpoints com abordagem proativa para resposta eficaz a incidentes	Por Endpoint	6800	R$ 292,00	R$ 1.985.600,00
2	Solução de proteção de Servidores com abordagem proativa para resposta eficaz a incidentes	Por Servidor	544	R$ 2.475,25	R$ 1.346.536,00
3	Solução de segurança avançada para mitigação de ameaças na rede	Por Throughput de dados	6	R$ 311.749,75	R$ 1.870.498,50
4	Solução de prevenção de intrusão de próxima geração (NGIPS)	Por Throughput de dados	1	R$ 1.006.500,00	R$ 1.006.500,00
5	Solução de Gerenciamento de Vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança.	Por dispositivos, assets, aplicações web, contêiner	20	R$ 596,45	R$ 11.929,00
6	Solução de Gerenciamento de Vulnerabilidades e Visibilidade de Ataques em tempo real para estrutura de Diretório de Usuários, com análise contínua e adaptável de riscos e confiança.	Por de usuários ativos no Active Directory	4300	R$ 709,50	R$ 3.050.850,00
7	Serviço de suporte pro ativo, corretivo e para resposta a incidentes	Por Solução	10	R$ 109.974,71	R$ 1.099.747,10
8	Serviço de implantação	Por Solução	10	R$ 22.850,43	R$ 228.504,30
9	Serviço de capacitação e repasse de conhecimento	40 Horas	4	R$ 21.750,00	R$ 87.000,00
10	Serviço de monitoramento do ambiente presencial	Por Posto	3	R$ 280.522,60	R$ 841.567 80

Item	Descrição do Item	Unidade de Medida	Quantidade	Valor Unitário	Valor Total
Custo Total Estimado					R$ 11.528.732,70

12.18. Por se tratar de licitação para Registro de Preços, os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens/serviços registrados, conforme disposto no Termo de Referência da Contratação.

13. JUSTIFICATIVA TÉCNICA DA ESCOLHA DA SOLUÇÃO

13.19. A escolha da solução abrangente, que inclui proteção de e-mail, Endpoint e proteção contra ataques avançados, está alinhada com as necessidades da SEAD-PI em garantir a segurança da rede para os usuários, prevenindo de forma proativa os ataques cibernéticos.

13.20. Existem benefícios significativos proporcionados por essa solução, como a capacidade de monitorar o comportamento das estações de usuários e caixas postais, detectar, bloquear, investigar e responder a incidentes de segurança da informação que possam ocorrer na rede da Secretaria. Além disso, essa solução está em conformidade com os requisitos de segurança da informação e atende às exigências da Lei Geral de Proteção de Dados (LGPD), o que evidencia que sua adoção trará melhorias significativas para o ambiente atual da Secretaria.

13.21. A adoção dessa solução trará benefícios em termos de qualidade e eficiência. Ela permitirá acompanhar as constantes evoluções dos recursos de TIC, ao mesmo tempo em que estará em conformidade com as exigências da LGPD.

13.22. A inclusão de serviços de instalação, configuração, suporte e garantia de atualização da solução por um período de 24 meses demonstra um compromisso com a qualidade e eficiência a longo prazo. Isso garantirá a disponibilidade e continuidade dos serviços de TI, além de fornecer suporte técnico especializado durante todo o período contratual.

13.23. Em resumo, a escolha dessa solução é justificada pela sua capacidade de garantir a segurança da rede, atender aos requisitos de segurança da informação, estar em conformidade com a LGPD e oferecer melhor qualidade, eficiência e suporte técnico especializado à SEAD-PI. Com essa escolha, a Secretaria estará protegendo seus sistemas e dados de forma abrangente e estará preparada para enfrentar os desafios da segurança cibernética de forma eficaz.

14. DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS TÉCNICOS

14.24. A solução proposta consiste em uma plataforma única e integrada de proteção de e-mail, Endpoint e proteção contra ataques avançados. Além disso, inclui serviços de instalação, configuração, suporte e garantia de atualização por um período de 24 meses.

14.25. Devido à natureza intrínseca e interdependente das funcionalidades e serviços oferecidos, não é viável parcelar a contratação por itens. É necessário que todos os componentes sejam fornecidos pelo mesmo fabricante e que os serviços sejam realizados por um profissional especializado na solução.

14.26. Após uma análise detalhada, a equipe de planejamento optou por adotar o modelo de contratação por menor preço global, separando a solução em itens. Essa abordagem garante a obtenção da solução completa, com todos os componentes e serviços necessários, assegurando a integridade e efetividade da solução proposta.

14.27. A escolha pelo modelo de contratação por menor preço global tem como objetivo garantir a qualidade, eficiência e cumprimento dos requisitos técnicos estabelecidos. Esse modelo assegura que todos os componentes e serviços estejam incluídos, permitindo que a solução funcione de maneira integrada e eficaz.

14.28. Portanto, a opção pelo modelo de contratação por menor preço global é justificada pela natureza integrada da solução, que requer a contratação conjunta de todos os seus componentes e serviços para garantir seu pleno funcionamento e eficácia.

15. JUSTIFICATIVA ECONÔMICA DA ESCOLHA DA SOLUÇÃO

15.29. A escolha da solução foi baseada não apenas em aspectos técnicos, mas também em uma análise econômica abrangente, levando em consideração não apenas o custo inicial da aquisição, mas também todos os custos associados ao longo do ciclo de vida da solução, conforme identificado no TCO (Custo Total de Propriedade).

15.30. Ao considerar os custos totais, incluindo instalação, configuração, suporte e garantia de atualização da solução por um período de 24 meses, bem como os custos de manutenção, atualização e treinamento, verifica-se que a solução escolhida oferece uma relação custo-benefício vantajosa. A integração completa das funcionalidades e serviços em uma única solução proporciona eficiência operacional, reduzindo a necessidade de recursos adicionais e simplificando a gestão e manutenção da infraestrutura de segurança cibernética. Isso resulta em economias significativas em termos de tempo, esforço e recursos humanos necessários para o gerenciamento da solução.

15.31. Além disso, a solução escolhida demonstrou ser altamente eficaz na detecção e remediação de ataques cibernéticos avançados, oferecendo proteção abrangente para as estações de trabalho contra ameaças comuns da internet, como vírus, worms, ransomware, keyloggers, backdoors, rootkits, trojans e spyware. Também oferece opções avançadas de bloqueio de dispositivos, garantindo a segurança dos sistemas e a proteção, integridade e autenticidade das informações. Isso garante o pleno funcionamento das atividades da SEAD-PI.

15.32. Considerando também as exigências da Lei Geral de Proteção de Dados (LGPD) e os requisitos de segurança da informação, a solução escolhida garante conformidade com as regulamentações, evitando possíveis penalidades e riscos legais que poderiam acarretar custos adicionais para a organização.

15.33. Portanto, a escolha da solução, levando em conta a análise econômica completa, demonstrou ser a opção mais vantajosa do ponto de vista financeiro. Além de oferecer um menor custo total de propriedade, ela também proporciona maior eficiência operacional, proteção abrangente contra ameaças cibernéticas e conformidade com as regulamentações aplicáveis.

16. DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS ECONÔMICOS

16.34. A decisão de não parcelar a contratação com base em aspectos econômicos é justificada pelos seguintes motivos:

16.35. A solução em questão é composta por funcionalidades e serviços intrinsecamente interligados. Isso significa que todos os componentes devem ser fornecidos pelo mesmo fabricante, e os serviços devem ser executados por um profissional especializado na solução. Parcelar a contratação

resultaria em uma complexidade adicional devido à necessidade de gerenciar vários fornecedores e garantir a compatibilidade e integração adequadas entre os componentes. Isso poderia aumentar os custos e comprometer a eficácia da solução.

16.36. O parcelamento da contratação não traria vantagens econômicas significativas. Pelo contrário, poderia resultar em custos adicionais, como a necessidade de coordenar diferentes contratos, lidar com possíveis incompatibilidades entre os componentes e arcar com os custos de integração. Ao optar por uma única contratação integrada, é possível obter um melhor custo-benefício, evitando gastos desnecessários e garantindo a eficiência operacional.

16.37. Ao optar por uma única contratação integrada, a gestão do contrato e dos serviços relacionados se torna mais simples e eficiente. É possível ter um único ponto de contato e responsabilidade, facilitando o monitoramento, a comunicação e a resolução de problemas. Isso reduz a necessidade de recursos dedicados à administração de múltiplos contratos e contribui para a otimização dos custos operacionais.

16.38. Portanto, levando em consideração a integração dos componentes, a falta de vantagem econômica no parcelamento, a disponibilidade orçamentária e os ganhos de escala, bem como a simplificação da gestão, a opção de não parcelar a contratação é a mais adequada do ponto de vista econômico.

17. BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

17.39. Monitoramento contínuo dos endpoints da SEAD-PI em busca de atividades suspeitas. Isso garante uma segurança proativa e eficaz, permitindo a identificação e mitigação de ameaças antes que elas possam causar danos significativos à organização.

17.40. Detecção avançada de ameaças que outros sistemas de segurança podem não conseguir detectar. Por meio da análise comportamental dos endpoints, a solução pode identificar padrões suspeitos e agir de forma rápida e efetiva para lidar com os incidentes de segurança, reduzindo os danos potenciais à organização.

17.41. Resposta automatizada a incidentes, adotando medidas como bloquear o acesso ao endpoint infectado, isolá-lo da rede ou executar ações de limpeza para remover o malware. Essa resposta automatizada agiliza o tempo de resposta aos incidentes, minimizando o impacto na organização.

17.42. Análise forense aprofundada dos endpoints comprometidos. A solução é capaz de capturar registros de eventos, memória e arquivos, o que facilita a identificação da origem da ameaça e a implementação de medidas preventivas para evitar futuros incidentes no ambiente da organização.

17.43. Aumento da eficiência operacional: Ao automatizar a detecção e resposta a ameaças comuns, a solução de antivírus corporativa contribui para o aumento da eficiência operacional da equipe de segurança. Isso permite que os profissionais se dediquem a tarefas mais críticas e estratégicas, reduzindo a carga de trabalho e otimizando o uso dos recursos disponíveis.

18. PROVIDÊNCIAS A SEREM ADOTADAS

18.44. Não serão necessárias providências adicionais ou ajustes para a utilização da solução de segurança contratada.

19. JUSTIFICATIVA

19.1. De acordo com o art. 11, Inciso V, § 1º e 3º, da Instrução Normativa SGD/ME nº 94/2022, a equipe de planejamento da contratação avaliou minuciosamente o estudo de soluções viáveis para atender às demandas da SEAD-PI. Com base nessa análise, concluiu-se que o presente Estudo Técnico Preliminar é plenamente viável, considerando os requisitos de negócios, administrativos e técnicos que devem ser alcançados para garantir que a solução proposta seja adequada e capaz de atender de forma eficiente e eficaz às necessidades da instituição, assegurando assim a viabilidade do projeto.

20. DECLARAÇÃO DE VIABILIDADE

20.1. Diante da necessidade ímpar dos serviços de aquisição e implantação de soluções tecnológicas e prestação de serviços especializados, visando a conformidade e adequação à Lei Nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), do ambiente e operações dessa Secretaria de Administração do Piauí - SEAD-PI e, considerando as soluções de mercado viáveis e considerando que a gestão digital é medida prevista no Decreto nº 21.979 de 13 de abril de 2023, que institui a Política de Transformação Digital do âmbito do Poder Executivo do Estado, Decreto Estadual nº 22.249, de 25 de julho de 2023, que institui a Política Estadual de Segurança da Informação e Comunicação do Estado do Piauí - POSIC, tem-se por concluído este estudo pela viabilidade da contratação.

20.2. A fiscalização do novo contrato deverá ser efetuada por Fiscal de Contrato a ser designado, o qual deverá ser servidor efetivo da Administração Pública e possuir experiência necessária para a gestão e acompanhamento de contratos de serviços que são objeto deste Estudo Técnico Preliminar.

20.3. Dessa forma, e considerando o conjunto de informações apresentadas, conclui-se pela viabilidade da contratação, sob o aspecto técnico e sob o aspecto econômico-financeiro, pelos benefícios almejados e, principalmente, o alcance dos objetivos institucionais com eficiência.

ANEXO I ESPECIFICAÇÃO TÉCNICA

21. DESCRIÇÃO DOS ITENS E QUANTITATIVOS

21.1. Solução de segurança para proteção de e-mail, Endpoint e proteção contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, para atender às necessidades dos órgãos e entes da Administração Pública, pelo período de 24 meses.

Item	Descrição do Item	Unidade de Medida	Quantidade
1	Solução de proteção de Endpoints com abordagem proativa para resposta eficaz a incidentes	Por Endpoint	6800
2	Solução de proteção de Servidores com abordagem proativa para resposta eficaz a incidentes	Por Servidor	544
3	Solução de segurança avançada para mitigação de ameaças na rede	Por Throughput de dados	6
4	Solução de prevenção de intrusão de próxima geração (NGIPS)	Por Throughput de dados	1
5	Solução de Gerenciamento de Vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança.	Por dispositivos, assets, aplicações web, contêiner	20

Item	Descrição do Item	Unidade de Medida	Quantidade
6	Solução de Gerenciamento de Vulnerabilidades e Visibilidade de Ataques em tempo real para estrutura de Diretório de Usuários, com análise contínua e adaptável de riscos e confiança.	Por de usuários ativos no Active Directory	4300
7	Serviço de suporte pro ativo, corretivo e para resposta a incidentes	Por Solução	10
8	Serviço de implantação	Por Solução	10
9	Serviço de capacitação e repasse de conhecimento	40 Horas	4
10	Serviço de monitoramento do ambiente presencial	Por Posto	3

22. **SOLUÇÃO DE PROTEÇÃO DE ENDPOINTS COM ABORDAGEM PROATIVA PARA RESPOSTA EFICAZ A INCIDENTES (ITEM 1)**

22.1. Características gerais

22.1.1. A solução deverá ser entregue na modalidade como um serviço (em nuvem);

22.1.2. Possuir console Web para gerenciamento e administração da ferramenta;

22.1.3. A proteção para estações de trabalho deverá prover Anti-Malware, Firewall, Host IPS, Controle de Aplicações e Controle de dispositivos em um único agente.

22.2. Módulo de Proteção Anti-Malware

22.2.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

- Windows 8.1 (x86/x64);
- Windows 10 (x86/x64);
- Windows 11 (x64).

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

22.2.3. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros;

22.2.4. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em: Processos em execução em memória principal (RAM);

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

22.2.6. Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, MIME/uu, CAB;

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

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

22.2.9. Deve possuir detecção heurística de vírus desconhecidos;

22.2.10. Deve permitir configurar o consumo de CPU que será utilizada para uma varredura manual ou agendada; Deve permitir diferentes configurações de detecção (varredura ou rastreamento):

22.2.11. Em tempo real de arquivos acessados pelo usuário;

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

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

22.2.14. Automáticos do sistema com as seguintes opções:

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

22.2.16. Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);

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

22.2.18. Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados. Deve possuir mecanismo de cache de informações dos arquivos já escaneados;

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

22.2.20. Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;

22.2.21. Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URL’s maliciosas, de modo a prover, rápida detecção de novas ameaças;

22.2.22. Deve ser capaz de aferir a reputação das URL’s acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independentemente da maneira de como a URL está sendo acessada;

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

22.2.24. Deve possuir capacidade de escaneamento de arquivos compactados e, em caso de identificação de um arquivo malicioso, apenas este deve ser removido, mantendo os demais intactos

22.2.25. Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;

22.2.26. Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;

22.2.27. Deve permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos;

22.2.28. Deverá ter funcionalidade de Machine Learning para detectar e tomar ações sobre ameaças desconhecidas e suspeitas;

22.2.29. Deverá ter funcionalidade de Machine Learning em runtime para evitar possíveis métodos de obfuscação que o módulo de Machine Learning em pré-execução não consiga detectar;

22.2.30. Deve fornecer um informativo compreensivo de cada simulação que descreva as ações e respectivos metadados, bem como, o porquê do veredito emitido pela Machine Learning;

22.2.31. Deve bloquear processos comuns associados a ransomware;

22.2.32. Em casos de ataques de ransomware, a solução deve ter a capacidade de interromper o processo de criptografia e restaurar os arquivos originais aos seus respectivos diretórios

22.2.33. Deve possuir funcionalidade de detecção de malwares conhecidos e desconhecidos por comportamento; Deve permitir a integração com solução de análise de artefatos suspeitos (sandbox) do próprio fabricante.

22.3. **Funcionalidade de Atualização**

22.3.1. Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;

22.3.2. Deve permitir atualização incremental da lista de definições de vírus;

22.3.3. Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;

22.3.4. Deve permitir o rollback das atualizações das listas de definições de vírus e engines;

22.3.5. Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utiliza-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;

22.3.6. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;

22.3.7. O agente replicador de atualizações e configurações, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização.

22.4. Funcionalidade de Administração

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

22.4.2. Deve possibilitar instalação "silenciosa";

22.4.3. Deve permitir o bloqueio por nome de arquivo;

22.4.4. Deve permitir o travamento de pastas e diretórios;

22.4.5. Deve permitir o travamento de compartilhamentos;

22.4.6. Deve permitir o rastreamento e bloqueio de infecções;

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

22.4.8. Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;

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

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

22.4.11. Deve permitir a deleção dos arquivos quarentenados;

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

22.4.13. Deve permitir integração com serviço de autenticação como Active Directory para acesso a console de administração;

22.4.14. Deve permitir criação de diversos perfis e usuários para acesso a console de administração;

22.4.15. Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

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

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

22.4.18. Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

22.4.19. Deve registrar no sistema de monitoração de eventos da console de anti-malware informações relativas ao usuário logado no sistema operacional;

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

22.4.21. Deve prover criptografia para as comunicações entre o servidor e os agentes de proteção; Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;

22.4.22. Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor de antivírus e o controlador de domínio;

22.4.23. Deve permitir a criação de usuários locais de administração da console de anti-malware;

22.4.24. Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de anti-malware;

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

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

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

22.4.28. Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido na console de administração;

22.4.29. Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto.

22.5. Funcionalidade de Controle de Dispositivos

22.5.1. As configurações da funcionalidade de controle de dispositivos devem ser aplicadas por usuário;

22.5.2. Deve permitir políticas e ações diferentes para dispositivos conectados à rede interna e aqueles utilizados na rede externa (conectado à Internet, por exemplo);

22.5.3. Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total;

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

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

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

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

22.5.8. Para ação de restrição como o bloqueio, a solução deve permitir adicionais dispositivos USB autorizados, bem como apontar executáveis específicos como exceção ao bloqueio;

22.5.9. Deve ter a capacidade de bloquear a função de Autorun nos dispositivos;

22.5.10. Deve permitir controle de permissão ou bloqueio para dispositivos que não armazenam dados tendo, pelo menos, os seguintes tipos de dispositivos: adaptadores bluetooth, dispositivos de imagem, modems, interfaces wireless externas, cartões PCMCIA, dispositivos infravermelhos e portas COM/LPT.

22.6. **Módulo de Proteção Anti-Malware para estações MacOS**

22.6.1. O cliente para instalação deverá possuir compatibilidade com os sistemas operacionais:

- macOS 12 (Monterey);
- macOS 11 (Big Sur) macOS 10.15 (Catalina);
- macOS 10.14 (Mojave); macOS 10.13 (High Sierra);

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

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

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

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

22.6.6. Permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus; Permitir a ações de reparar arquivo ou colocar em quarentena em caso de infeções a arquivos;

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

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

- Proteção e verificação dos arquivos de assinatura;
- Proteção dos processos do agente de segurança;
- Proteção das chaves de registro do agente de segurança;
- Proteção do diretório de instalação do agente de segurança.

22.7. **Funcionalidade de HIPS – Host IPS e Host Firewall**

22.7.1. Deve ser capaz de realizar a detecção/proteção contra exploração de vulnerabilidades nos seguintes sistemas operacionais:

- Windows 11 (x64).

- Windows 10 (x86/x64);
- Windows 8.1 (x86/x64);

22.7.2. Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPS e host firewall;

22.7.3. As regras de vulnerabilidades deverão possuir a opção de desativar a regra de forma individual;

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

22.7.5. Deve permitir ativar e desativar o produto sem a necessidade de remoção;

22.7.6. Deve permitir que o usuário altere as configurações de níveis de segurança e exceções;

22.7.7. Deverá possuir a possibilidade de configurar níveis diferentes de segurança podendo ser eles alto, médio e baixo;

22.7.8. O modulo de HIPS deverá possuir perfis pré-determinados baseados em performance e segurança; O modulo de HIPS deverá possuir regras pra proteger contra ameaças do tipo Ransomware;

22.7.9. O modulo de HIPS deverá conter regras contra exploit, vulnerabilidades e genericas protegendo contra ameaças conhecidas ou desconhecidas;

22.7.10. O módulo de HIPS deverá permitir que o administrador monitore apenas ou realize o bloqueio das tentativas de exploração de vulnerabilidades;

22.7.11. Deve suportar configuração de parâmetros de pacotes como quantidade máxima de conexões TCP e timeout para pacotes UDP;

22.7.12. Deve ter a capacidade de proteção contra exploração de vulnerabilidades do sistema operacional e de aplicações terceiras instaladas na estação de trabalho;

22.7.13. A lista de regras deve permitir que o administrador realize buscas e tenha rápida visibilidade do tipo da aplicação, em que modo a regra encontra-se (bloqueio ou monitoramento), CVE, CVSS score, quando aplicável.

22.8. **Módulo para Controle De Aplicações**

Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

22.8.1. Windows 8.1 (x86/x64);

22.8.2. Windows 10 (x64);

22.8.3. Windows 11 (x64).

22.8.4. As regras de controle de aplicação devem permitir as seguintes ações:

22.8.4.1. Permissão de execução;

22.8.4.2. Bloqueio de execução;

22.8.4.3. Bloqueio de novas instalações.

22.8.5. A regra de liberação para o controle de aplicação deverá permitir que o programa liberado efetue ou não a execução de outros processos,

22.8.6. As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;

22.8.7. As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações:

22.8.7.1. Assinatura SHA-1 e SHA-256 do executável;

22.8.7.2. Atributos do certificado utilizado para assinatura digital do executável;

22.8.7.3. Caminho lógico do executável;

22.8.7.4. Base de assinaturas de cortiçados digitais válidos e seguros.

22.8.8. As regras de controle de aplicação devem possuir categorias pré-determinadas de aplicações;

22.8.9. As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações;

22.8.10. O módulo de controle de aplicativos deve possuir uma lista de aplicações mal-intencionados para bloqueio e monitoramento tendo, pelo menos, as categorias de KeyLoggers, anonimizadores de proxy, P2P, crackers de senhas;

22.8.11. Deve permitir a busca por aplicações ou fabricante destas;

22.8.12. Deve possuir ferramenta para extrair o hash de um ou um grupo de executáveis, permitindo a importação destes hashes através de arquivo CSV.

22.9. **Módulo de Detecção e Resposta**

22.9.1. A solução deve ser compatível com os sistemas operacionais Windows, Linux e MacOS;

22.9.2. O fabricante deve implementar e organizar os ataques baseados no framework MITRE ATT&CK®, identificando técnicas e táticas dos ataques;

22.9.3. A solução deve possuir módulo de investigação e detecção integrados;

22.9.4. Deve fazer uso de inteligência artificial e inteligência de ameaças do fabricante da solução para analisar e correlacionar as atividades dos sensores do ambiente;

22.9.5. Possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nos usuários, aplicações acessadas e estações de trabalho;

22.9.6. Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;

22.9.7. Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;

22.9.8. Fornece a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;

22.9.9. Capacidade de construir sequências de buscas poderosas para localizar os dados ou objetos em seu ambiente que você deseja examinar;

22.9.10. Deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta do tipo Kibana para identificar, categorizar e recuperar os resultados da pesquisa;

22.9.11. Deve ser possível realizar buscas através de strings parciais, exatas, valores nulos, wildcards e caracteres especiais;

22.9.12. Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;

22.9.13. Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;

22.9.14. Deve permitir que as detecções sejam correlacionadas com módulos de servidores, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;

22.9.15. A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;

22.9.16. Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;

22.9.17. O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos; Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;

22.9.18. A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;

22.9.19. A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;

22.9.20. Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;

22.9.21. Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;

22.9.22. Deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, como pontuações ou níveis de prioridade;

22.9.23. Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;

22.9.24. Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;

22.9.25. Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta;

22.9.26. Deve destacar e organizar as atividades relacionadas a cada modelo de detecção por ordem cronológica, permitindo identificar a relação de cada atividade com os modelos de detecção;

22.9.27. Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;

22.9.28. Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada estação de trabalho;

22.9.29. Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;

22.9.30. Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;

22.9.31. A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);

22.9.32. Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas;

22.9.33. Deve informar qual o escopo de impacto ou dimensionar o impacto em servidores, estações de trabalho e usuários, indicando a quantidade de componentes afetados no ataque;

22.9.34. Deve permitir que o analista possa alterar o status dos incidentes de acordo com seu tratamento e indicar falsos positivos para a plataforma;

22.9.35. Deve permitir adicionar arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores; Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores; Deve permitir terminar processos ativos executados nas estações de trabalhos e servidores; Permitir coletar e fazer o download de um arquivo para investigação local detalhada;

22.9.36. Isolar a estação de trabalho desconectando-a da rede e permitindo se comunicar exclusivamente com a console de gerenciamento do fabricante;

22.9.37. Restaurar a conectividade da estação de trabalho com a rede;

22.9.38. Iniciar uma sessão de shell remoto na estação de trabalho selecionada para execução de comandos remotos para investigação;

22.9.39. Deve ser possível fazer o download do histórico da sessão após finalizar a sessão remota do shell na estação de trabalho para fins de auditoria.

23. SOLUÇÃO DE PROTEÇÃO DE SERVIDORES COM ABORDAGEM PROATIVA PARA RESPOSTA EFICAZ A INCIDENTES (ITEM 2)

23.1. SOLUÇÃO DE SEGURANÇA PARA CARGAS DE TRABALHO HÍBRIDAS COM DETECÇÃO E RESPOSTA, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO

23.1.1. Características Gerais Da Solução

23.1.1.1. A solução deverá ser compatível com pelo menos os seguintes sistemas operacionais:

- Windows Server 2000; Windows Server 2003 SP1 e 2003 R2 SP2; Windows Server 2008 e 2008 R2; Windows Server 2012 e 2012 R2; Windows Server 2016; Windows Server 2019; Windows Server 2022;
- Red Hat Enterprise 5, 6, 7 e 8;

- CentOS 5, 6, 7 e 8; AIX 6.1, 7.1 e 7.2; Oracle Linux 5, 6, 7 e 8; SUSE Linux Enterprise Server 10, 11, 12 e 15; Ubuntu 10, 12, 14, 16, 18 e 20; Debian 6, 7, 8, 9 e 10; Rocky Linux 8; Alma Linux 8;
- Cloud Linux 5, 6, 7 e 8; Solaris 10 1/13 Sparc; Solaris 10 1/13 (x86/x64); Solaris 11.2/ 11.3 Sparc; Solaris 11.2/ 11.3 (x86/x64);Solaris 11.4 (x86, x64 ou SPARC) Amazon Linux e Amazon Linux 2 (x64).

23.1.1.2. A solução deverá ser totalmente compatível e homologada com o ambiente Vmware;

23.1.1.3. A console de gerenciamento deverá ser em nuvem, permitindo o gerenciamento das políticas de segurança através da Internet;

23.1.1.4. A solução deverá ser gerenciada por console Web, compatível com pelo menos os browsers Internet Explorer, Google Chrome e Firefox. Deve ainda suportar certificado digital para gerenciamento;

23.1.1.5. A solução deverá permitir a integração com pelo menos as seguintes plataformas de nuvem: Vmware vCloud, MS Azure e AWS;

23.1.1.6. Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console única e centralizada do próprio fabricante;

23.1.1.7. A solução deverá permitir a entrega de agentes por pelo menos duas dentre as principais ferramentas de distribuição de software do mercado: Microsoft System Center Configuration Manager, Novel Zen Works e Puppet;

23.1.1.8. A console de administração deverá permitir o envio de notificações via SMTP;

23.1.1.9. Todos os eventos e ações realizadas na console de gerenciamento precisam ser gravados para fins de auditoria;

23.1.1.10. A solução deverá possuir a funcionalidade tags para identificar falsos positivos ou facilitar a visualização de determinados alertas;

23.1.1.11. A solução deverá permitir a criação de widgets para facilitar a administração e visualização dos eventos;

23.1.1.12. A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;

23.1.1.13. A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob- demanda, ou agendado com o envio automático do relatório via e-mail;

23.1.1.14. A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos PDF, CSV, XLS e RTF;

23.1.1.15. A solução precisa permitir que relatórios no formato PDF, possam ser enviados com uma senha única para cada destinatário;

23.1.1.16. A solução deverá prover relatórios contendo no mínimo as seguintes informações; malware, regras de IPS aplicadas e Firewall;

23.1.1.17. Em caso de solução e nuvem, o ambiente do fabricante deverá fornecer alta disponibilidade; A solução de segurança ter a capacidade de identificar ataques entre conteineres;

23.1.1.18. Os usuários devem ter a capacidade de receber determinados papéis para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial";

23.1.1.19. Quando configurado o acesso parcial, este deve permitir que um usuário tenha permissões de poder gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível ou não editar ou criar novas políticas de segurança;

23.1.1.20. A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;

23.1.1.21. Cada agente deverá ter sua própria chave para criptografia de modo que a comunicação criptografada seja feita de forma diferente para cada agente;

23.1.1.22. A console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;

23.1.1.23. Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL/TLS com o servidor de onde ela buscará as informações;

23.1.1.24. Os agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de script PowerShell;

23.1.1.25. Os agentes para plataforma Linux deverão ser instalados por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de bash script;

23.1.1.26. Em servidores Windows e Linux, a solução deverá permitir a atualização automática dos agentes após sua ativação;

23.1.1.27. Para servidores Linux, a solução deverá possibilitar a atualização automática da versão quando o agente reiniciar;

23.1.1.28. Para efeito de administração, a solução deverá avisar quando um agente se encontrar não conectado a sua console de gerenciamento;

23.1.1.29. Deve permitir a remoção automática de agentes inativos, definindo o período para, pelo menos 1 semana, 1 mês e 12 meses;

23.1.1.30. A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;

23.1.1.31. Cada perfil poderá ser atribuído para um host ou um conjunto de hosts;

23.1.1.32. A solução deverá vir com perfis pré-definidos e aptos a funcionarem de acordo com sua denominação; A solução deverá mostrar quais máquinas estão usando determinada política;

23.1.1.33. Os agentes deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e após isso deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;

23.1.1.34. Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;

23.1.1.35. A solução deverá permitir a configuração de componentes de integração com o vCenter, a fim de permitir a sincronização das máquinas virtuais conectadas a ele;

23.1.1.36. Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;

23.1.1.37. O administrador do sistema de segurança deverá ter a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host;

23.1.1.38. A solução deve possuir a capacidade de isolamento de placa de rede de forma que apenas uma fique funcionando de acordo com preferência do administrador;

23.1.1.39. A solução deverá ser capaz de aplicar políticas diferentes para placas de redes diferentes em um mesmo servidor;

23.1.1.40. A solução deverá ser capaz de executar bypass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;

23.1.1.41. A solução deverá ter a capacidade de se integrar com o Amazon SNS e os principais softwares de SIEMs contemplando, no mínimo: Splunk, IBMQradar e HPArcSight de modo a permitir enviar os seus logs para essas soluções;

23.1.1.42. A solução deverá ter a possibilidade de enviar logs para SYSLOG servers;

23.1.1.43. Solução deverá permitir criar relatórios customizados de todas as suas funcionalidades;

23.1.1.44. Deve permitir enviar os relatórios para uma lista de contatos independente de login na console de administração;

23.1.1.45. As atualizações de assinaturas deverão ocorrer de forma agendada e automática possibilitando ser até mesmo de hora em hora;

23.1.1.46. Após a atualização deve ser informado o que foi modificado ou adicionado;

23.1.1.47. Deve ser possível baixar as assinaturas na console de gerenciamento, mas não as distribuir aos clientes;

23.1.1.48. A console de gerenciamento deve apresentar a capacidade de gerar roll back de suas atualizações de regras;

23.1.1.49. A solução deverá ter capacidade de gerar pacote de autodiagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;

23.1.1.50. Deverá ter a capacidade de colocar etiquetas para a ocorrência de determinados eventos de modo a facilitar o gerenciamento, relatórios e visualização;

23.1.1.51. No gerenciamento de licenças, deve ser informada quantidade contratada e quantidade em utilização de clientes;

23.1.1.52. Solução deverá ter mecanismo de procura em sua console de gerenciamento de modo que seja facilitada a busca de regras;

23.1.1.53. Deverá possuir a capacidade de classificar eventos para que facilite a identificação e a visualização de eventos críticos em servidores críticos;

23.1.1.54. Deverá possibilitar colocar etiquetas em eventos para que se possam visualizar apenas os eventos desejados;

23.1.1.55. O fabricante deverá participar do programa “Microsoft Application Protection Program” para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante;

23.1.1.56. A console de gerenciamento deve se integrar com o Vmware vCloud, de modo a importar e sincronizar os objetos (hosts vmware e guests vm) para a console de gerenciamento da solução;

23.1.1.57. O fabricante da solução deverá manter programa de pesquisa em vulnerabilidades há, pelo menos, 5 anos; A solução deve possuir API documentada para integração na esteira de automação;

23.1.1.58. A documentação da API deve conter exemplos prontos para implementação de determinadas funcionalidades, como cookbooks;

23.1.1.59. Precisa ter a capacidade de detectar e aplicar as regras necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;

23.1.1.60. A solução deve permitir desabilitar os módulos individualmente;

23.1.1.61. Precisa ter a capacidade de desabilitar as regras não mais necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador.

23.1.2. **Antimalware**

23.1.2.1. A solução deve permitir a proteção contra códigos maliciosos através da instalação 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;

23.1.2.2. A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do SO;

23.1.2.3. A solução deve possuir listas de exclusão separadas por módulo da proteção antimalware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;

23.1.2.4. Em plataforma Windows, a solução deve permitir criar exclusões de escaneamento a partir do certificado digital das aplicações;

23.1.2.5. A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção. A limpeza deve ocorrer sem a descompactação do arquivo;

23.1.2.6. Em servidores Windows, deve identificar e bloquear ameaças através de métodos de Machine Learning, quarentenando arquivos identificados;

23.1.2.7. A solução deverá possuir a funcionalidade de Monitoramento de Comportamento para detectar mudanças e atividades suspeitas não autorizadas;

23.1.2.8. A solução deverá oferecer escanear processos em memória em busca de Malware;

23.1.2.9. O scan de arquivos comprimidos deverá ser de no mínimo 6 camadas de compressão;

23.1.2.10. O scan de arquivos comprimidos do tipo OLE deverá ser de no mínimo 20 camadas de compressão;

23.1.2.11. Para servidores Windows, a solução deverá permitir que o escaneamento agendado ocorra, ainda que o agente esteja offline na console de gerenciamento;

23.1.2.12. A solução deverá possuir ações pré-configuradas para cada tipo de ameaça detectada ou tomar uma ação baseada na configuração padrão da ferramenta;

23.1.2.13. Em servidores Windows, a solução deverá integrar-se com interface AMSI (Antimalware Scan Interface);

23.1.2.14. A solução deverá mostrar informação de data sobre o último scan agendado ou manual executado; Possuir a capacidade de efetuar backup e restore de arquivos comprometidos por Ransomware; Deve possuir cache dos arquivos verificados de modo a evitar a redundância da varredura;

23.1.2.15. Deve possibilitar o controle do consumo de memória durante as varreduras a fim de minimizar os impactos de desempenho no servidor;

23.1.2.16. A solução deve possuir opção para forçar a comunicação com o agente e coletar os respectivos logs; Em servidores Windows, deve possuir capacidade de detectar ameaças por comportamento;

23.1.2.17. Deverá ter a possibilidade de escanear drivers de rede mapeados nos servidores.

23.1.3. **Proteção Contra URLs Maliciosas**

23.1.3.1. Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação;

23.1.3.2. 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;

23.1.3.3. A solução deve permitir alterar o nível de sensibilidade para detecção de URLs maliciosas tendo, pelo menos, os níveis Alto, médio e baixo;

23.1.3.4. Deve permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema;

23.1.3.5. Deve permitir configurar notificações personalizadas para detecções desse módulo, deixando a cargo do administrador exibir ou não tais notificações;

23.1.3.6. Deverá ter capacidade de identificar acessos a URLs maliciosas além das portas padrão 80 e 443;

23.1.3.7. A solução deve permitir que o administrador reclassifique uma URL através do site do fabricante para evitar falsos positivos;

23.1.3.8. A proteção deve possibilitar proteção através da instalação de agente de segurança do fabricante da solução de segurança.

23.1.4. **Firewall**

23.1.4.1. Operar como firewall de host, através da instalação de agente nos servidores protegidos;

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

23.1.4.3. Precisa ter a capacidade de controlar conexões TCP baseado nas Flags TCP; Precisa ter a capacidade de definir regras distintas para interfaces de rede distintas;

23.1.4.4. A solução deverá ser capaz de reconhecer e possibilitar o bloqueio endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP FYNSYN Scan, TCP Xmas Scan e Computer OS FIngerprint por até 30 minutos;

23.1.4.5. Precisa ter a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;

23.1.4.6. Precisa ter a capacidade de definição de regras para contextos específicos;

23.1.4.7. Para facilitar a criação e administração de regras de firewall, as mesmas poderão se apoiar em objetos que podem ser lista de ips, lista de MACs, lista de portas;

23.1.4.8. Regras de firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não);

23.1.4.9. Regras de firewall poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana; O firewall deverá ser stateful bidirecional;

23.1.4.10. O firewall deverá permitir liberar ou apenas logar eventos;

23.1.4.11. O firewall deverá ser passível de criação de regras através do protocolo, origem do tráfego, frame type, TCP header flags, destino e direção;

23.1.4.12. As regras de Firewall deverão ter as seguintes ações, ou equivalentes: Allow, log only, bypass, force allow, deny;

23.1.4.13. A solução, para facilidade de administração, deverá utilizar o conceito de regras implícitas para a regra ALLOW, negando o tráfego para todo o restante que não estiver liberado;

23.1.4.14. As ações também deverão ser possíveis de terem prioridades diferentes, sendo que a prioridade maior prevalece sobre a prioridade menor;

23.1.4.15. Deverá realizar pseudo stateful em tráfego UDP; Deverá logar a atividade stateful;

23.1.4.16. Deverá permitir limitar o número de conexões entrantes e o número de conexões de saída de um determinado computador;

23.1.4.17. Deverá permitir limitar o número de meias conexões vindas de um computador; Deverá prevenir ack storm;

23.1.4.18. Deverão existir regras default que possam ser utilizadas como modelo para a criação e adição de novas regras;

23.1.4.19. Deverá identificar escaneamentos ativos de porta ou da rede, bloqueando o IP ofensor por um período de tempo configurado pelo administrador;

23.1.4.20. Deverá permitir criar lista de exceções para identificar os Ips autorizados a realizar varreduras de portas ou da rede;

23.1.4.21. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

23.1.5. **Proteção De Vulnerabilidades de SO e Aplicações**

23.1.5.1. Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;

23.1.5.2. Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do SO, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada;

23.1.5.3. A solução deverá conter regras pré-definidas para detecções de ransomware para as principais famílias deste tipo de malware;

23.1.5.4. Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão;

23.1.5.5. Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows 2003, 2008, 2012, 2016, 2019, Linux Red Hat, Suse, CentOS, Ubuntu, Debian, Solaris, AIX além de regras para aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache;

23.1.5.6. Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;

23.1.5.7. Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;

23.1.5.8. Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e instant Messaging;

23.1.5.9. Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injection e Cross Site Scripting. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para

23.1.5.10. fins de investigação do incidente;

23.1.5.11. Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;

23.1.5.12. Ser capaz de permitir ou negar que métodos utilizados por Webservers por regras de IPS;

23.1.5.13. Regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não);

23.1.5.14. Regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana; Deverá ser capaz de inspecionar tráfego criptografado de entrada;

23.1.5.15. Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: SQL injection, Crossite script, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, Double Decoding Exploit;

23.1.5.16. As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;

23.1.5.17. Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo, bloquear acesso a um determinado website ou bloquear acesso de uma aplicação X;

23.1.5.18. Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;

23.1.5.19. Deverá 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 uma determinada web browser ou aplicação de backup;

23.1.5.20. Solução deve ser capaz de habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;

23.1.5.21. As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;

23.1.5.22. As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;

23.1.5.23. As regras de IPS de vulnerabilidade deverão apresentar severidade baseada em CVEs; As regras de IPS poderão ter sua capacidade de LOG desabilitado;

23.1.5.24. As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta; As regras devem ser atualizadas automaticamente pelo fabricante;

23.1.5.25. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

23.1.6. **Monitoramento De Integridade**

23.1.6.1. A solução deverá permitir a implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX, através da instalação de agentes;

23.1.6.2. Precisa ter a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;

23.1.6.3. Precisa ser capaz de detectar mudanças no estado de portas em sistemas operacionais Linux; Precisa ter a capacidade de monitorar o status de serviços e processos do sistema operacional; Precisa ter a capacidade de monitorar mudanças efetuadas no registro do Windows;

23.1.6.4. Precisa ter a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e customização de XML para criação de regras avançadas;

23.1.6.5. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de monitoramento de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;

23.1.6.6. O monitoramento poderá ser realizado em tempo real ou utilizando de scans periódicos para detectar mudanças de integridade;

23.1.6.7. Deverá alertar toda vez que uma modificação ocorrer em tempo real para ambiente Windows e pseudo real-time para ambiente Linux;

23.1.6.8. Deverá logar e colocar em relatório todas as modificações que ocorram;

23.1.6.9. As regras de monitoramento de integridade deverão ser atualizadas pelo fabricante ou melhoradas de forma automática;

23.1.6.10. Deverá poder classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;

23.1.6.11. Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;

23.1.6.12. Algumas regras podem ser modificadas pelo administrador para adequação ao seu ambiente.

23.1.7. **Inspeção De Logs**

23.1.7.1. A solução deverá permitir sua implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX;

23.1.7.2. Precisa ter a 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;

23.1.7.3. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de inspeção de logs de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;

23.1.7.4. Precisa permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;

23.1.7.5. Precisa permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;

23.1.7.6. Deverá rastrear e indicar/sugerir ao administrador do sistema quais softwares estão instalados e que possuem logs passíveis de inspeção;

23.1.7.7. Deverá possibilitar a criação de regras de inspeção de logs para aplicações customizadas;

23.1.7.8. Deverá ter inteligência para que a cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente ou do servidor seja alertada;

23.1.7.9. Deverá ter inteligência para que a cada violação relevante no log inspecionado que seja suspeita no servidor seja alertada;

23.1.7.10. Deverá logar cada violação e colocar em relatório todas as violações relevantes que ocorram; As regras poderão ser modificadas por severidade de ocorrência de eventos;

23.1.7.11. As regras devem se atualizar automaticamente pelo fabricante;

23.1.7.12. Permitir modificação pelo administrador em regras para adequação ao ambiente.

23.1.8. **Controle De Aplicações**

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

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

23.1.8.3. O agrupamento dos eventos deverá ser realizado pelo menos por Hash ou por máquina; A console deverá exibir eventos de no mínimo 30 dias;

23.1.8.4. A solução deverá possuir um mecanismo ao qual permita a execução de aplicações e scripts automaticamente, sem intervenção manual, por um determinado período que deve ser no máximo 10 horas;

23.1.8.5. A solução deverá possuir no mínimo as funcionalidades de bloquear o que não for permitido explicitamente e permitir o que não for bloqueado explicitamente.

23.1.9. **Detecção e Resposta**

23.1.9.1. A solução deve ser compatível com Linux e Windows Server 2008 R2 e superiores; A solução deve possuir módulo de investigação, detecção integrados;

23.1.9.2. Deve permitir que as detecções sejam correlacionadas com módulos de endpoint, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;

23.1.9.3. A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;

23.1.9.4. Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;

23.1.9.5. O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos; Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;

23.1.9.6. A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;

23.1.9.7. A solução deve permitir realizar buscas em todos os dados de atividades enviadas pelos servidores e demais sensores que estejam conectados na console, ainda que estas não sejam detectadas como maliciosas;

23.1.9.8. A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;

23.1.9.9. Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;

23.1.9.10. Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;

23.1.9.11. Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;

23.1.9.12. Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada servidor;

23.1.9.13. Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;

23.1.9.14. Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;

23.1.9.15. A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);

23.1.9.16. Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.

24. SOLUÇÃO DE SEGURANÇA AVANÇADA PARA MITIGAÇÃO DE AMEAÇAS NA REDE (ITEM 3)

24.1. **SOLUÇÃO DE SEGURANÇA CONTRA AMEAÇAS AVANÇADAS COM DETECÇÃO E RESPOSTA, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 24 MESES**

24.1.1. **Características Gerais**

24.1.1.1. A solução deverá ser instalada de modo a detectar ameaças avançadas no ambiente da CONTRATANTE, inspecionando o tráfego de rede, independente de agentes instalados;

24.1.1.2. Funcionalidades e Requisitos específicos:

24.1.1.3. Deverá fornecer solução integrada de proteção contra ameaças avançadas de acordo com funcionalidades e características técnicas especificadas neste documento, contendo, no mínimo os seguintes módulos:

24.1.1.4. Monitoramento, Identificação, Análise e Resposta de Incidentes de Segurança;

I - Detecção de ataques direcionados;

II - Analisador virtual de ameaças;

III - Correlação de regras para detecção de conteúdo malicioso;

IV - Análise de todos os estágios de uma sequência de ataques.

24.1.2. Esta solução deverá ser atendida através do fornecimento de solução de um único Fabricante, contendo:

24.1.2.1. Serviço de Monitoração e Análise de Ameaças Digitais em rede;

24.1.2.2. Serviço de Monitoração e gestão de riscos que permita a identificação de ameaças digitais conhecidas e não conhecidas por soluções de antivírus tradicionais, permitindo a composição de serviços de mitigação complementares para a segurança do ambiente;

24.1.2.3. Serviço que entenda ameaça digital como a representação de um software malicioso ou ação maliciosa tal como: spyware, phishing, worms, bot, trojan, adware, network Exploit, web Exploit, Cross-site scripting, spear phishing, information stealing malware e outras ações que podem compor ataques ao patrimônio computacional do ambiente;

24.1.2.4. Visibilidade e relatório de incidentes de conexões da rede interna com sites maliciosos ou servidores de central de comando (C&C) externos;

24.1.2.5. Análise e correlação de atividades maliciosas tais como: Detecção específica de malwares conhecidos e arquivos contaminados através de assinaturas de antivírus tradicional no tráfego da rede; Detecção de vermes de rede e de e-mail no tráfego de rede; Detecção de programas de exploração de vulnerabilidades (Exploits) na rede; Detecção de empacotamentos maliciosos no tráfego da rede;

24.1.2.6. Validação de tráfego web malicioso através de consultas a sistemas de reputação na Internet;

24.1.2.7. Visibilidade e relatório de estatísticas de ameaças, fontes de infecção na rede monitorada e máquinas comprometidas.

24.1.2.8. Permitir a rápida identificação da criticidade dos eventos de segurança

24.1.2.9. Permitir realizar pesquisas avançadas e customizadas dos incidentes de segurança através da console de gerenciamento;

24.1.2.10. Possibilidade de criação de filtros para visualização de eventos específicos conforme contexto, localização e outras variáveis que permitam investigação profunda sobre causa raiz de incidentes de segurança;

24.1.2.11. Permitir a customização de alertas em base ao tipo de incidente de segurança através da console de gerenciamento;

24.1.2.12. Permitir a integração com sistemas de serviço de diretório;

24.1.2.13. Capacidade de verificar em tempo real a reputação de endereços web (URL's) e servidores de correio SMTP;

24.1.2.14. A análise de SMTP poderá ser realizada em uma solução separada do sensor de HTTP e demais protocolos;

24.1.2.15. A capacidade de análise de artefatos em sandbox pode ser realizada através de no mesmo equipamento de análise;

24.1.2.16. A solução deverá possuir mecanismo de conhecimento de senhas de pelo menos 90 palavras chaves em

24.1.2.17. seu vocabulário de conhecimento, para derivação de arquivos protegidos; Capacidade de criar e salvar investigações customizadas dos incidentes de segurança;

24.1.2.18. Deve possuir pelo menos 1 sensor para inspecionar o tráfego de rede de throughput de 04Gbps de análise;

24.1.2.19. Deve possuir a capacidade de detectar ameaças direcionadas, ataques do dia zero e documentos que viabilizem ataques;

24.1.2.20. Deve detectar atividades maliciosas que trafegam na rede através de motor de análise de comportamento de tráfego até o nível 7 (camada de aplicação) em protocolo TCP/IP;

24.1.2.21. Capacidade de detectar ameaças web tais como vulnerabilidades e download de conteúdo malicioso;

24.1.2.22. Os módulos de captura de rede deverão suportar a coleta de arquivos pelo menos nos protocolos HTTP e HTTPS;

24.1.2.23. Deve possuir a habilidade de detectar e analisar os seguintes protocolos e aplicativos: P2P, SMTP, POP3, IRC, DNS, HTTP, FTP, TFTP, SMB, MSN, AIM, YMSG, Yahoo Mail, Hotmail, RDP, DHCP, TELNET, File Transfer, VNC, Cisco-TELNET, Kerberos, DCE-RPC, SQL, HTTPS, SMB2, MMS, IMAP4, RTSP/RTP-UDP, RTSP/RTP-TCP, RTSP/RDT-UDP, RTSP/RDT-TCP, WMSP, SHOUTCast, RTMP,

24.1.2.24. Bittorent, Kazaa, Blubster, eDonkeyeMule, Gnucleus LAN, Gnutella/Limewire/Bearshare/Shareaza, Winny, WinMX, MLDonkey, DirectConnect, SoulSeek, OpenNap, Kuro, iMesh, Skype, Google Talk, Zultrax, Foxy, eDonkey, Ares, Miranda, Kceasy, MoodAmp, Deepnet Explorer, FreeWire, Gimme, GnucDNA GWebCache, Jubster, MyNapster, Nova GWebCache, Swapper GWebCache, Xnap, Xolox, Ppstream, AIM Express, Chikka SMS Messenger, eBuddy, ICQ2Go, ILoveIM Web Messenger, IMUnitive, mabber, meebo, Yahoo Web Messenger, GPass, IP, ARP, TCP, UDP e IGMP;

24.1.2.25. Deve possuir capacidade de disponibilizar facilmente as amostras dos arquivos suspeitos detectados e do arquivo PCAP do contexto de captura;

24.1.2.26. Capacidade de oferecer informações para análise forense de artefatos suspeitos de serem maliciosos;

24.1.2.27. Gerenciamento centralizado de todas as etapas dos eventos de segurança identificados como possíveis ameaças;

24.1.2.28. Capacidade de identificar artefatos maliciosos direcionados para dispositivos moveis rodando o sistema operacional Android, tais como telefones inteligentes e tablets;

24.1.2.29. Deve analisar em tempo real o comportamento através de simulação de execução de arquivos provenientes do tráfego de rede incluindo arquivos PDF´s, executáveis, PPT, DOC, XLS, ZIP e RAR;

24.1.2.30. A solução deve detectar ameaças do dia zero, vulnerabilidade, URL's maliciosas e spams dirigidos no protocolo SMTP;

24.1.2.31. Deve possuir tecnologia de análise de arquivos binários através de simulação e avaliação de execução dos artefatos suspeitos para identificação de comportamento malicioso, com capacidade de operar vários ambientes simultâneos e integrados a solução para processamento de alto desempenho;

24.1.2.32. Deve permitir o uso de base de conhecimento na Internet do próprio fabricante para correlacionamento de informações sobre ameaças conhecidas e prover recomendações de ações;

24.1.2.33. Deve permitir o uso de portas espelhadas de switch (mirror port) para monitorar o tráfego e detectar potenciais riscos à Segurança;

24.1.2.34. Deverá permitir o rastreio por malwares utilizando métodos de detecção baseados no tipo de arquivo (True File Type), múltiplas camadas de empacotamento (Multi-packed/Multi-layered files) e arquivos comprimidos (compactados);

24.1.2.35. Deverá analisar arquivos maliciosos na rede utilizando vacinas e técnicas de heurística; Deve possuir foco em proteção contra APTs (Advanced Persistent Threats);

24.1.2.36. Deve possuir tecnologia de proteção contra ameaças desconhecidas (ataques dirigidos e ameaças de dia zero), sendo que este módulo deve pertencer ao mesmo fabricante;

24.1.2.37. Deverá possuir suporte para monitorar múltiplas interfaces de rede conectadas a diferentes VLANs ou witches;

24.1.2.38. Deverá possuir suporte para balanceamento de carga no sensor de inspeção de tráfego, possibilitando assim obter uma melhor performance;

24.1.2.39. Deverá permitir a análise específica de eventos de segurança de computadores suspeitos de atividade maliciosa;

24.1.2.40. Os módulos que compõem a solução devem atuar de forma integrada, centralizando logs de incidentes em ponto único;

24.1.2.41. Deve possuir atualização automática de regras e assinaturas, sendo que estas devem ser disponibilizadas via web pelo fabricante da solução;

24.1.2.42. Deve possuir mecanismo de consultas automáticas em bases de reputação externas de propriedade do fabricante da solução;

24.1.2.43. Deve ser capaz de identificar movimentos laterais em uma rede corporativa;

24.1.2.44. Deve atuar de forma passiva na captura de tráfego sem oferecer impacto no desempenho da rede; Deve possuir interface web para busca e investigação local de incidentes;

24.1.2.45. O ambiente controlado de sandbox deve contemplar, pelo menos, os sistemas operacionais CentOS, Windows 10, Windows 7, Windows Server 2003, 2008, 2012 R2, 2016 e 2019;

24.1.2.46. Deve possuir possibilidade de habilitação e desabilitação de regras de inspeção, individualmente, através de interface de gerenciamento web;

24.1.2.47. Deve possuir regras que identifiquem comunicações dos seguintes tipos: C&C, Exploits, Executáveis Maliciosos, Comunicação com Sites Maliciosos, backdoors e Botnets;

24.1.2.48. Deve possuir regras que identifiquem comunicações de estações de trabalho e servidores com serviços não autorizados, tais como: consultas DNS em servidor não autorizado, utilização de SMTP server não autorizado, Proxy Server não autorizado;

24.1.2.49. Deve possuir regras que identifiquem comunicações p2p, instant messengers e streaming;

24.1.2.50. Deve possuir capacidade de geração de relatórios dos seguintes tipos e contendo as seguintes características:

I - Resumidos;

II - Visão Geral dos Incidentes de Segurança Discriminação dos Tipos de Incidentes Top Ameaças Analisadas

III - Top Hosts Infectados Recomendações de Segurança Executivos;

IV - Deve possuir detalhes técnicos dos incidentes detectados;

V - Deve possuir estatística do tráfego analisado;

VI - Deve possuir indicadores de risco do ambiente; Recomendações de Segurança.

24.1.2.51. Deve ser capaz de identificar, filtrar e exibir em interface gráfica, e dinamicamente atualizada, hosts com alto nível de risco, classificando os tipos de riscos/eventos detectados;

24.1.2.52. Deve possuir interface que apresente em Real Time estatísticas de top ameaças detectadas, top arquivos analisados, top hosts afetados, top URL's maliciosas acessadas, etc.;

24.1.2.53. Quando detectada uma ameaça, a solução deve prover, podendo esta realizar consultas em site do fabricante, informações sobre ameaça, família da ameaça, estatísticas de segmentos de mercado afetados e recomendações de segurança para eliminar ameaça, correlacionando estas informações com sites ou outros vetores por onde esta ameaça é disseminada;

24.1.2.54. As atualizações do produto (patterns e outros componentes) não devem causar downtime ou impacto na operação;

24.1.2.55. Deve ser capaz de identificar ameaças que afetam dispositivos móveis (Ex. Detecção de comunicação de aplicativo malicioso na plataforma Android);

24.1.2.56. Deve ser capaz de detectar tentativas de mascaramento ou evasão de detecção através do uso de portas comuns ou protocol tunneling;

24.1.2.57. Deve ser capaz de detectar tentativas de scan de rede;

24.1.2.58. Deve ser capaz de detectar propagação de malwares na rede; Deve ser capaz de detectar tentativas de brute-force;

24.1.2.59. Deve ser capaz de detectar tentativas de fuga e roubo de informação; Deve ser capaz de detectar ameaças que se replicam na rede;

24.1.2.60. Deve ser capaz de detectar Exploits na rede;

24.1.2.61. O Monitoramento de protocolos de comunicação deve ser feito através de appliance único (ou virtual appliance);

24.1.2.62. A console de gerenciamento deve possuir mapa mundial, onde são marcadas origens de ataques e eventos de segurança monitorados pela solução;

24.1.2.63. Deve permitir busca por informações do destino e origem, incluindo estas: endereço IP, endereço MAC, porta e protocolo;

24.1.2.64. Deve permitir consultas personalizáveis, usando comandos SQL ou atributos pré-definidos; Capacidade de salvar uma investigação antes de ser finalizada;

24.1.2.65. Capacidade de restaurar uma investigação para continuá-la ou consultá-la; Capacidade de emitir relatórios baseados nas investigações;

24.1.2.66. Deve permitir apresentação dos dados consultados em vários formatos, incluindo tabela e gráficos; Deve trabalhar com geo-localização para identificar a origem geográfica de um ataque;

24.1.2.67. Deve ter a capacidade de sugerir termos de busca, de acordo com o conteúdo já buscado numa investigação, para agilizar a obtenção do resultado;

24.1.2.68. Deve permitir exportar sob demanda os logs em texto puro (CSV ou similar);

24.1.2.69. Deve sugerir consultas a bases de reputação e whois quando encontrados hosts e nomes de domínio; Deve permitir investigação por tags (palavras-chave) pré-configuradas para facilitar a busca de eventos; Deve permitir recebimento de logs via syslog;

24.1.2.70. Deve permitir encaminhamento de logs via syslog; Deve permitir receber logs de diferentes dispositivos; Deve possuir engine de correlação de eventos;

24.1.2.71. Deve inserir tags personalizadas nos logs, de acordo com regras especificadas pelo usuário;

24.1.2.72. A solução de análise em sandbox deve ter a capacidade de analisar, de forma estática e dinâmica, ameaças com características de autoinicialização ou alteração de arquivos de sistema, rootkits/cloakings, arquivos mal-formados, engenharia social, dentre outros;

24.1.2.73. A análise de sandbox deve identificar e analisar ameaças que tenham características de evitar a segurança e análise em sandbox, e auto-preservação;

24.1.2.74. Deve enviar alertas via e-mail para pelo menos 100 e-mails diferentes;

24.1.2.75. Deve permitir a configuração de alarmes personalizados, com base em investigações;

24.1.2.76. Deve informar em sua console alarmes que dispararam, até que o usuário tome alguma ação;

24.1.2.77. A console de gerenciamento deverá ser web, apresentando alta disponibilidade de modo que na ausência da principal, o restante da solução permaneça ativa e funcionando;

24.1.2.78. A solução deve ser escalável horizontalmente, permitindo que novas instâncias sejam habilitadas, aumentando suas capacidades de detecção e analise;

24.1.2.79. A console de gerenciamento deverá ter dashboards para facilidade de monitoração. As janelas deverão ser customizadas pelo administrador em quantidade e período de monitoração;

24.1.2.80. O administrador deve poder optar por janelas de monitoramento no dashboard a sua disposição e poderá livremente adicionar ou remover de acordo com sua necessidade de visualização;

24.1.2.81. Deverá possuir mapa geográfico que permita a identificação visual sobre a origem de ameaças de modo a facilitar a visualização de eventos críticos para que ações imediatas sejam providenciadas;

24.1.2.82. Deverá possuir a capacidade de atualizar as vacinas, engines, assinaturas e recursos de inspeção de conteúdo de forma agendada e automática;

24.1.2.83. A console de gerenciamento deverá ser gerenciada por Internet Explorer, Google Chrome e Firefox;

24.1.2.84. Solução deverá ter mecanismo de busca em sua console de gerenciamento de modo que seja facilitada a busca por detecções;

24.1.2.85. Deverá ser capaz de identificar ameaças evasivas em tempo real com o provimento de análise profunda e inteligência para identificar e prevenir ataques;

24.1.2.86. Deverá ser capaz de correlacionar regras de detecção de conteúdo malicioso durante todas as fases de um ataque;

24.1.2.87. Deve permitir a adição e remoção dos diversos recursos de visualização de informações na tela principal de monitoramento da ferramenta, permitindo no mínimo a visualização das seguintes informações:

I - Uso de CPU Uso de Disco;

II - Uso de Memória;

III - Tráfego malicioso analisado;

IV - Todo o tráfego analisado.

24.1.2.88. A solução deverá permitir o envio de logs dos recursos para servidor de logs por meio do protocolo syslog e deverá conter no mínimo:

I - Tipo de evento de detecções: Conteúdo malicioso, reputação de URL’s, comportamentos maliciosos, comportamentos suspeitos, Exploits, correlações de eventos, Grayware;

24.1.2.89. Tipo de eventos de sistemas:

I - Eventos de sistema e eventos de atualizações.

24.1.2.90. A solução deverá ter integração com ferramentas de SIEM;

24.1.2.91. Deve possuir capacidade de entregar relatório contendo informações da sequência de execução do artefato malicioso, assim como, detalhes de alterações locais da máquina, conexões externas e envio da informação para fora da rede corporativa;

24.1.2.92. A solução deve prover serviço de agregação e correlação de logs de eventos de segurança possibilitando coleta de fontes de monitoração para proporcionar informação e identificação de ameaças digitais conhecidas e desconhecidas em transito através de logs de sensor;

24.1.2.93. Solução deverá apresentar relatórios customizados de todas as suas funcionalidades e deverá conter no mínimo:

I - Computadores infectados;

II - Origem de infecções;

III - Estatísticas de ameaças;

IV - Riscos potenciais de segurança;

V - Riscos de perda de informações;

VI - Risco de sistema comprometido;

VII - Risco de disseminação de ameaças;

VIII - Eventos suspeitos;

IX - Infecções de malware.

24.1.2.94. A solução deverá apresentar função de pesquisa por logs contendo no mínimo:

I - Critérios de pesquisa por dia, mês e ano.

II - Possibilidade de pesquisa pelo nome do computador, domínio ou conta, endereço IP, endereço MAC e grupos;

24.1.2.95. Possibilidade de pesquisa por ameaças, URL's maliciosas, análises virtuais, correlação de incidentes, nome de malware, protocolo e direção da detecção;

24.1.2.96. Os relatórios e logs deverão ser exportados nos formatos PDF ou CSV.

24.1.3. **Módulo de Detecção e Resposta**

24.1.3.1. A solução deve ter a capacidade de integrar-se com a plataforma de investigação e resposta centralizada, a fim de enviar objetos suspeitos e metadados das detecções locais para correlação com as demais soluções de segurança do ambiente;

24.1.3.2. A funcionalidade deve ser licenciada para analisar o throughput total do appliance;

24.1.3.3. A solução deve permitir a integração dos eventos ocorridos em outros segmentos de rede e outros appliances com objetivo de correlacionar os ataques na rede;

24.1.3.4. Deve permitir a análise em linha de tempo gráfica, representando a sequência da comunicação dos ativos, bem como seu protocolo e direção;

24.1.3.5. Deve identificar tentativas de ataques avançados na rede da CONTRATANTE e correlacionar com eventos das soluções de estação de trabalho, servidores e e-mail, a fim de rastrear o passo-a-passo do ataque na rede;

24.1.3.6. Caso necessário, a CONTRATANTE pode optar em direcionar parte do licenciamento deste módulo para outros módulos da plataforma de Detecção e Resposta, como o monitoramento do email, endpoint ou servidores, sem acréscimos ou mudanças de licenciamento;

24.1.3.7. Ao clicar em um dos objetos identificados pela solução de inspeção de rede, a plataforma deverá informar um resumo do ataque em questão, contendo o IP/hostname envolvido, quais protocolos, atividades maliciosas, severidade do incidente, fases do ataque;

24.1.3.8. Deve exibir de forma e em tabela, as transações identificadas contendo detalhes do ataque, bem como os Indicadores de Comprometimento (IOCs).

25. SOLUÇÃO DE PREVENÇÃO DE INTRUSÃO DE PRÓXIMA GERAÇÃO (NGIPS) (ITEM 4)

25.1. Plataforma e Performance

25.1.1. A solução NGIPS (NEXT GENERATION INTRUSION PREVENTION SYSTEM) ofertada deverá ser disponibilizada em hardware do próprio fabricante, não sendo aceitos hardwares de fabricantes terceiros, não sendo aceitos também hardwares homologados (quando o fabricante da solução-software e do hardware são empresas diferentes);

25.1.2. Não serão aceitas soluções NGFW ou UTM;

25.1.3. O NGIPS deverá suportar a importação de regras no padrão SNORT, podendo esta ocorrer de forma direta e nativa via interface de gerenciamento, ou então através de ferramenta de conversão, onde o arquivo padrão SNORT deverá ser importado e convertido para o padrão utilizado pela solução ofertada;

25.1.4. A solução NGIPS deverá possuir interfaces de rede modularizadas com, pelo menos, 2 slots para inserção de módulos;

25.1.5. Os módulos disponíveis para a solução NGIPS devem contemplar, pelo menos, expansão até 20 interfaces 10/100/1000Gbps;

25.1.6. Para atendimento do bypass das interfaces cobre, não serão aceitos dispositivos externos. Nas interfaces de fibra óptica deverá ser ofertado módulo de bypass, que poderá ser embutido ou externo;

25.1.7. A solução NGIPS deverá usar discos de estado sólido (SSD), não sendo aceitos equipamentos com discos mecânicos;

25.1.8. Deverá ser entregue equipamento NGIPS que atenda às seguintes especificações:

25.1.8.1. IPS com throughput de inspeção de 5Gbps;

25.1.8.2. Deverá gerar latência igual ou inferior a 40 Microsegundos; Deverá suportar pelo menos 390.000 novas conexões por segundo; Deverá suportar pelo menos 29 milhões de sessões concorrentes;

25.1.8.3. Deverá suportar pelo menos 3.300 novas conexões SSL por segundo; Deverá suportar inspeção de tráfego SSL de até 3,5Gbps;

25.1.8.4. O hardware ofertado deverá possuir fontes redundantes do tipo hot-swap; O hardware ofertado deverá operar entre 0°C até 40°C;

25.1.8.5. O hardware ofertado deverá operar em ambientes com umidade entre 5% e 95%.

25.2. **Requisitos Técnicos e de Segurança**

25.2.1. A solução NGIPS ofertada deverá prover funcionalidades de prevenção de intrusão, em seu modo default (configuração básica) com pelo menos 2000 regras ativas (habilitadas automaticamente quando uma nova política de segurança é criada, em modo bloqueio e com criação de notificação);

25.2.2. A solução NGIPS ofertada deverá prover funcionalidades de prevenção de intrusão, em seu modo default (configuração básica) com pelo menos 2000 regras ativas (habilitadas automaticamente quando uma nova política de segurança é criada, em modo bloqueio e com criação de notificação);

25.2.3. Os filtros providos pelo NGIPS deverão permitir a seleção de ações de resposta. Deverão existir pelo menos as seguintes ações: Block (drop packet), Block (TCP Reset), Permit, Trust, Notify, Trace (Captura de Pacotes), além de ações condicionais, que permitam a definição de ações que alternam entre permitir e bloquear determinados tráfegos / ataques de acordo com condições encontradas no ambiente como, por exemplo, permitir as 1000 primeiras conexões de um único IP para determinado tráfego de rede em um período de 15 minutos. Após a conexão 1001 na mesma janela de tempo, a ação deverá ser alternada para bloqueio;

25.2.4. A solução NGIPS deverá suportar assinaturas de IPS para proteger vulnerabilidades, detectar exploits, detectar roubo de informações, detecção de virus, detecção de spywares, detectar tentativas de reconhecimento de rede, possuir regras que ajudem a controlar comportamentos de rede (exemplo: permitir ou bloquear resposta de comandos ping, detectar falhas de autenticação no MS SQL Server), possuir regras que blindem equipamentos de rede contra ataques que explorem vulnerabilidades, regras que efetuem a normalização de tráfego, ou seja, detectem tunelamento de protocolos, e cabeçalhos IP incompletos, além de filtros que permitam e detecção e controle de aplicações, tais como youtube, skype, TOR e facebook;

25.2.5. Os filtros do NGIPS precisam estar segmentados por categorias, com o objetivo de facilitar o gerenciamento da solução. Deverão existir pelo menos as seguintes categorias: Políticas de Segurança, Exploits, Normalização de Tráfego, Vírus, Reconhecimento de Rede, P2P e Vulnerabilidades;

25.2.6. O total de filtros disponíveis na solução (não necessariamente para uso simultâneo) não deve ser inferior a 16.000;

25.2.7. A solução NGIPS deverá ser capaz de permitir a criação e uso de políticas de segurança granulares baseados nos seguintes métodos:

25.2.8. Por NGIPS (todos os segmentos de rede de um IPS);

25.2.9. Por segmento físico, podendo selecionar o modo bi-direcional ou unidirecional (permitindo ativar a política de segurança nos sentidos de comunicação de A > B e de B > A [na mesma politica de segurança]. Ou com política de segurança dedicada de A > B e também de B > A);

25.2.10. Por TAG de VLAN (802.1Q), de forma direcional e bi-direcional; Por CIDR (Range de endereços IP);

25.2.11. Baseado no horário do dia.

25.2.12. A solução NGIPS deverá ser capaz de detectar e bloquear ataques de reconhecimento de rede;

25.2.13. A solução NGIPS deverá prover filtros de detecção de aplicações tais como P2P, Online Games, permitindo a ativação de controles de banda;

25.2.14. Deverá possuir ferramenta para criação de filtros customizados, sendo que estes deverão permitir a customização de parâmetros tais como:

25.2.15. Nome do filtro; Descrição do filtro;

25.2.16. Protocolo, permitindo a criação de filtros de proteção baseados nos protocolos IPv4, ICMPv4, UDP, TCP, HTTP, IPv6 e ICMPv6;

25.2.17. Severidade do filtro, devendo possuir pelo menos 4 níveis; Customização da categoria do filtro;

25.2.18. Classe do filtro (devendo possuir pelo menos as classes DoS, Exploit, Virus e Acesso);

25.2.19. Gatilhos de acionamento (triggers), onde parâmetros ou informações/dados contidos no streaming de rede serão utilizados como gatilho para validação de parâmetros adicionais da regra;

25.2.20. Detecção de payload, permitindo o uso de strings e expressão regular para detecção avançada de instruções no streaming de rede;

25.2.21. Detecção de payload dentro do protocolo HTTP, permitindo o uso de strings e expressão regular para buscar e validar a existência de informações no cabeçalho HTTP, distinguindo métodos GET, POST, OPTIONS, PUT, DELETE, TRACE, CONNECT, HEAD, LOCK, UNLOCK, PROPFIND. Também

25.2.22. deverá permitir a validação de dados específicos em URI, URI PATH, URI Target, Header e Payload;

25.2.23. Criação de customizações a nível TCP, sendo possível definir portas de origem e destino, além de validação de flags TCP;

25.2.24. A solução NGIPS ofertada deverá suportar processamento de tráfego assimétrico; Deverá ser possível colocar a solução em modo bypass total forçado;

25.2.25. A solução NGIPS deverá possuir Machine Learning, ou seja, deverá possuir filtros que implementem Machine Learning na detecção de, por exemplo, conteúdo obfuscado em HTML associado/relacionado a exploit kits;

25.2.26. Deverá possuir filtros de gerenciamento de tráfego, ou seja, deverá ser possível criar regras para controlar o tráfego no sentido de A para B, de B para A, liberando o tráfego (com inspeção de riscos de segurança), liberando o tráfego (sem inspecioná-lo, confiando na conexão), bloqueando o tráfego, e também permitindo a criação de políticas de controle de banda, permitindo limitar, por exemplo, determinado fluxo de dados de rede a 100kbps;

25.2.27. A solução de NGIPS deverá possuir controles de proteção contra ataques de DDOS, atuando como um SYN PROXY;

25.2.28. A solução de NGIPS deverá possuir filtros que detectem a tentativa de uso de TOR, TeamViewer; A solução de NGIPS deverá detectar e bloquear tráfego Skype;

25.2.29. A solução de NGIPS deverá detectar e permitir o bloqueio de tunelamento de conexões DNS;

25.2.30. A solução de NGIPS deverá possuir assinatura que permita a validação de requisições HTTP 2.0; A solução de NGIPS deve bloquear nativamente a transferência de arquivos maliciosos via FTP;

25.2.31. A solução deve detectar ataques baseados em SSL, como por exemplo detectar o uso de certificados SSL/TLS maliciosos.

25.3. **Atualizações de Segurança**

25.3.1. A solução de NGIPS ofertada precisa entregar detalhes sobre a cobertura para vulnerabilidades Microsoft reportadas nos últimos 12 meses;

25.3.2. O fabricante da solução NGIPS deve prover estatísticas do número de vulnerabilidades de dia zero descobertas nos últimos 5 anos.;

25.3.3. O fabricante da solução NGIPS deverá possuir times de pesquisa de vulnerabilidades de dia zero e de riscos de segurança, com pelo menos 1500 pesquisadores, sejam contratados ou parceiros, sendo que deverão ser apresentadas estatísticas dos últimos 3 anos de vulnerabilidades pesquisadas e descobertas. O fabricante deverá estar entre os Top 5 maiores pesquisadores do mundo nos relatórios publicados pela entidade Frost & Sullivan (Analysis of the Global Public Vulnerability Research);

25.3.4. A solução NGIPS deverá suportar atualizações automáticas dos filtros/assinaturas, possuindo frequência de atualizações mínima semanal (fabricante deverá entregar 1 atualização por semana);

25.3.5. Sempre que a solução NGIPS atualizar-se, o novo pacote de atualizações deverá conter descritivo visualizável na própria solução (console local do NGIPS ou gerenciamento centralizado), indicando quais filtros foram incluídos, quais foram modificados e quais foram removidos. O mesmo deve ocorrer para os filtros de ameaças (malwares), sendo exigidos os mesmos parâmetros para permitir o acompanhamento e monitoramento dos novos filtros adicionados pela solução.

25.4. **Correlação de Informações e Consultas em Nuvem**

25.4.1. Reputação de Endereços IP, DNS e URLs;

25.4.2. A solução NGIPS ofertada precisa permitir o bloqueio de tráfego baseado na reputação do endereço de IP de origem da conexão, de destino da conexão, através da reputação de DNS e URLs;

25.4.3. O serviço de reputação deverá contar com categorias tais como: Malware, Botnet, Spyware, SPAM, TOR, Web, Application Attackers, P2P e Network Worm;

25.4.4. Deverá ser possível criar exceções baseadas em domínio e endereços IP, assim como deverá ser possível estabelecer as políticas de reputação individuais para cada perfil de segurança em uso no ambiente;

25.4.5. A base de reputação IP deverá suportar IPv4 e IPV6;

25.4.6. A base de reputação IP deverá ser baseada em informações do próprio fabricante, e também permitir o uso de bases terceiras;

25.4.7. Os filtros de reputação de IP deverão atuar tanto no sentido inbound quanto outbound;

25.4.8. As políticas de reputação deverão permitir a customização de ações tanto para bloquear ou permitir determinados acessos;

25.4.9. Deverá ser possível criar filtros de controle de acesso inbound e outbound baseados em geolocalização.

25.5. **Proteção Avançada Contra Ameaças**

25.5.1. A solução NGIPS deverá possuir funcionalidade que permita a identificação e proteção contra atividades maliciosas relacionadas a virus e spywares, no sentido inbound e outbound;

25.5.2. A solução NGIPS deverá possuir assinaturas de proteção contra malwares;

25.5.3. As assinaturas de malware deverão detectar a infiltração, exfiltração e comunicação com servidores de

25.5.4. comando e controle através da inspeção do tráfego de rede;

25.5.5. A solução deverá ser capaz de interromper atividades maliciosas tais como ransomware, fuga de dados, click fraud, etc;

25.5.6. Deverá bloquear ameaças do tipo drive-by-downloads;

25.5.7. Deverá detectar atividades de comunicação com servidores de comando e controle de botnets; Os filtros de malware deverão ser atualizados de forma regular pelo fabricante da solução.

25.6. **Alta Disponibilidade**

25.6.1. A solução de NGIPS deve suportar a operação de forma redundante, com possíveis cenários de operação Ativo-Passivo e Ativo-Ativo;

25.6.2. A gerência da solução deve permanecer ativa em caso de indisponibilidade dos NGIPS e possui cenários de alta disponibilidade;

25.6.3. A solução NGIPS ofertada deverá suportar fontes do tipo hot-swappable; A solução NGIPS deverá suportar software bypass;

25.6.4. Em caso de atualizações ou reinicializações do NGIPS, a solução não deverá gerar nenhuma interrupção de rede.

25.7. **Gerenciamento Centralizado**

25.7.1. A solução NGIPS precisa suportar ser gerenciada de maneira centralizada por solução fornecida pelo mesmo fabricante;

25.7.2. A solução de gerenciamento centralizado entregue deverá permitir o gerenciamento de pelo menos 4 equipamentos NGIPS, sendo possível efetuar os mesmos níveis de configuração existentes na solução NGIPS;

25.7.3. A solução NGIPS deverá permitir integração com ferramentas de monitoramento de rede e SIEM tais como, HP ArcSight, além de permitir o envio de alertas por e-mail notificando incidentes de segurança;

25.7.4. A solução de gerenciamento centralizado deverá possuir um painel de monitoramento de eventos, contendo pelo menos as estatísticas dos principais filtros acionados, principais atacantes, principais alvos dos ataques etc.;

25.7.5. A solução de gerenciamento centralizado deverá permitir a integração com dispositivos de rede, tais como switchs e roteadores, com recursos que permitam alterar a configuração de VLAN de portas de rede, e desligar determinada porta de um switch de rede. Este recurso poderá ser utilizado para contenção de incidentes internos de segurança;

25.7.6. A solução de gerenciamento centralizado deverá possuir API que permita soluções externas, como o próprio SIEM, a interagir com a solução NGIPS, devendo permitir pelo menos a adição e remoção de endereços IP suspeitos em listas de reputação, e permitindo adicionar e remover endereços IP suspeitos da quarentena dos NGIPS;

25.7.7. A solução de gerenciamento centralizado deverá possuir recurso para relacionar relatórios de testes de penetração realizados no ambiente da empresa, permitindo comparar tais relatórios com políticas de segurança em uso, indicando quais regras ou filtros são necessários ativar para alinhar a política de segurança com as vulnerabilidades identificadas no ambiente;

25.7.8. A solução deverá possuir suporte nativo a pelo menos as seguintes ferramentas: Qualys, Nessus e Nexpose;

25.7.9. A solução de gerenciamento centralizado deverá possuir módulo de relatórios próprio, possuindo templates que indiquem os principais riscos de segurança detectados no ambiente, contando com pelo menos 20 modelos pré-estabelecidos. Deverá ser possível agendar o envio destes relatórios, sendo exigidos no mínimo os seguintes formatos de arquivo: PDF, DOCX, XLS, CVS e XML;

25.7.10. A solução de gerenciamento centralizado deverá suportar o gerenciamento paralelo de pelo menos 4 IPS. A solução ofertada deverá estar dimensionada para atender o exigido neste edital, com crescimento suportado previsto para até 20 NGIPS;

25.7.11. A solução de gerenciamento centralizado deverá permitir a integração com soluções de Sandboxes (detecção de ameaças desconhecidas) de modo a permitir que URLs contendo executáveis sejam analisados e testados por soluções de sandboxes que devem ser do próprio fabricante, a fim de identificar novas ameaças direcionadas ao ambiente. Indicadores como endereços IP e DNS relacionados a novas ameaças devem ser passíveis de bloqueio através da própria solução NGIPS (solução de sandbox deverá fazer o feedback dos indicadores relacionados a novas ameaças);

25.7.12. A solução de gerenciamento centralizado deverá possuir dashboard que permita a adição ou remoção de painéis que serão utilizados no monitoramento do ambiente, indicando os hosts comprometidos, hosts vulneráveis que sofreram ataques, lista de objetos suspeitos com quantidades de hits identificados;

25.7.13. A solução de gerenciamento centralizado deverá permitir a integração com serviços de diretório, tendo suporte aos métodos de autenticação CAC, RADIUS, TACACS+ e Active Directory, além de autenticação local (para uso enquanto solução não é integrada com restante da infraestrutura);

25.7.14. A solução deverá ser fornecida em modo de alta disponibilidade, tendo pelo menos 2 nós de redundância;

25.7.15. Quando implementado em modo alta disponibilidade, a solução de gerenciamento centralizado deverá permitir a operação usando IP Virtual;

25.7.16. A solução de gerenciamento deverá possuir API que permita que soluções terceiras interajam podendo por exemplo quarantenar determinado endereço IP, desquarentenar determinado endereço IP, inserir e remover endereços IP de uma lista de reputação;

25.7.17. A solução de gerenciamento centralizado deverá atuar como ponto central para o gerenciamento de políticas de IPS, devendo possuir versionamento de políticas, capacidade de rollback, além de capacidade de importação e exportação de configurações.

26. SOLUÇÃO DE GERENCIAMENTO DE VULNERABILIDADES PARA ENDPOINTS, BASEADA E COM ANÁLISE CONTÍNUA E ADAPTÁVEL DE RISCOS E CONFIANÇA (ITEM 5)

26.1. Solução de Gestão de Vulnerabilidade e Auditoria de Configurações de Ativos

26.1.1. A solução deve realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance);

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

26.1.3. A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;

26.1.4. A solução deve ser licenciada pelo número de endereços IP ou dispositivos (assets);

26.1.5. A solução deve fornecer um modelo de armazenamento integrado que não dependa de um banco de dados externos ou de terceiros;

26.1.6. Caso a solução dependa de banco de dados de terceiros, todas as licenças deverão ser fornecidas pela CONTRATADA.

26.1.7. A solução deverá suportar API (Application Programming Interface) baseada em REST (Representatonal State Transfer) para automação de processos e integração com aplicações terceiras.

26.1.8. A solução deve possuir integração via API no mínimo as seguintes linguagens: Python, Powershell, Ruby, javascript, Java, Swift e PHP;

26.1.9. A solução deve possuir métodos de consulta via api e envio, tais como: HTTP METHOD (POST, GET, PUT AND DELETE)

26.1.10. A solução deve incluir a opção para agentes instalados e licenciados em estações de trabalho e servidores, para varredura diretamente no sistema operacional;

26.1.11. Tais agentes devem ser gerenciados pela mesma interface/console da plataforma de gestão de vulnerabilidades;

26.1.12. A solução deve permitir o agrupamento de scanners para facilitar o gerenciamento e aplicação de políticas.

26.1.13. A solução deve realizar a varredura tanto de dispositivos na rede interna, dispositivos expostos a demais redes externas, tanto quanto dispositivos em nuvens públicas como Azure, AWS ou GCP.

26.1.14. O escaneamento para os dispositivos expostos deve sem realizados através de SCANS (ENGINE) do próprio fabricante alocados no Brasil;

26.1.15. Os scanners e sensores agentes deverão ser gerenciados por uma única plataforma, de maneira centralizada;

26.1.16. O acesso a console de gerenciamento deve ser fornecida para pelo menos 10 usuários simultâneos;

26.1.17. A solução deve ser capaz de se integrar e disponibilizar insumos para soluções de correlação de eventos externa (SIEM);

26.1.18. A solução deve apresentar, para cada vulnerabilidade encontrada, a descrição e passos que devem ser tomados para correção;

26.1.19. A solução deve apresentar, para cada vulnerabilidade encontrada, evidências da vulnerabilidade através de saídas das verificações (outputs);

26.1.20. A solução deve fornecer controle de acesso baseado em função (RBAC- Role Based Access Control) para controlar o acesso do usuário a conjuntos de dados e funcionalidades;

26.1.21. A solução deve ser capaz de definir e gerenciar grupos de usuários, incluindo limitação de funções de varreduras e acesso a relatórios e dashboards;

26.1.22. A solução deve ter a capacidade de excluir determinados endereços IP do escopo de qualquer varredura ou scan;

26.1.23. A solução deve criptografar todos resultados de varreduras obtidos e informações inseridas tanto em descanso quanto em trânsito;

26.1.24. A solução deve suportar métodos de autenticação usando bases de autenticação local, e SAML (Security Assertion Markup Language) para uso de SSO (Single Sign-On);

26.1.25. A solução deve ser capaz de orquestrar scanners ilimitados dentro da infraestrutura;

26.1.26. A solução não deve impor nenhum limite de quantidade de scanners implementados dentro da infraestrutura;

26.1.27. A solução deverá possuir sistema de alertas para informar a disponibilidade de resultados dos escaneamentos através de email e SMS;

26.1.28. A solução deve oferecer capacidade de configuração dinâmica de grupos de ativos através de no mínimo as seguintes características:

26.1.28.1. Sistema Operacional, Endereço IP, DNS, NetBIOS Host, MAC, AWS Instance Type, AWS EC2 Name, Software instalado,

26.1.28.2. Azure VM ID, AWS Region, Google Cloud Instance ID, Azure Resource ID, Ativos avaliados;

26.2. **Dos requisitos e relatórios e painéis gerenciais**

26.2.1. A solução deverá possuir painéis gerenciais (dashboards) pré-definidos para rápida visualização dos resultados, permitindo ainda a criação de painéis personalizados.

26.2.2. Os painéis gerenciais deverão ser apresentados em diversos formatos, incluindo gráficos e tabelas, possibilitando a exibição de informações em diferentes níveis de detalhamento.

26.2.3. Os relatórios devem ser disponibilizados sob demanda no console de gerência da solução;

26.2.4. Os relatórios devem conter informações da vulnerabilidade, severidade, se existe um exploit disponível e informações do ativo.

26.2.5. A solução deve permitir a customização de dashboards/relatórios;

26.2.6. A solução deve concentrar todos os relatórios na plataforma central de gerenciamento, não sendo aceitas soluções fragmentadas;

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

26.2.8. A solução deve possibilitar a criação de relatórios baseado nos seguintes alvos:

26.2.8.1. Todos os ativos e Alvos específicos;

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

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

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

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

26.3. **Das varreduras**

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

26.3.2. A solução deve suportar varredura com e sem agente, de maneira ativa e passiva, distribuídas em diferentes localidades e regiões e gerenciar todos por uma console central;

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

26.3.4. Tais agentes devem realizar conexões para o sistema gerenciamento através de protocolo seguro;

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

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

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

26.3.8. A solução deve se integrar com solução de gerenciamento de acessos privilegiados para autenticação nos dispositivos, no mínimo, os seguintes:

26.3.8.1. CyberArk;

26.3.8.2. BeyondTrust;

26.3.8.3. Thycotic;

26.3.8.4. Centrify.

26.3.8.5. Senhasegura

26.3.9. A solução deve suportar o agendamento de scans personalizados, incluindo a capacidade de executar varreduras em tempos designados, com frequência pré-determinada;

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

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

26.3.12. A solução deve ser capaz de realizar em tempo real a descoberta de vulnerabilidades nas seguintes tecnologias:

26.3.12.1. Cloud Services;

26.3.12.2. Data Leakage;

26.3.12.3. Database;

26.3.12.4. IoT;

26.3.12.5. Mobile Devices;

26.3.12.6. Operating System;

26.3.12.7. Peer-To-Peer;

26.3.12.8. SCADA;

26.3.12.9. Web Servers;

26.3.12.10. Web Clients.

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

26.3.14. A solução deve em tempo real, detectar logins e downloads de arquivos em um compartilhamento de rede.

26.4. **Da análise e priorização de vulnerabilidades**

26.4.1. A solução deve ser capaz de exibir ambos severidade e pontuação, com base em CVSS (Common Vulnerability Scoring System) e inteligência de ameaças;

26.4.2. A solução deve utilizar sistema de pontuação e priorização das vulnerabilidades que utilize no mínimo:

26.4.2.1. CVSS Impact Score;

26.4.2.2. Idade da Vulnerabilidade;

26.4.2.3. Maturidade de códigos de exploração da vulnerabilidade encontrada;

26.4.2.4. Frequência de uso da vulnerabilidade em ataques e campanhas atuais;

26.4.2.5. Disponibilidade do código de exploração da vulnerabilidade;

26.4.2.6. Presença de módulos de exploração de vulnerabilidade em frameworks automatizados de exploração de vulnerabilidades como CANVAS, Metasploit e Core Impact;

26.4.2.7. Popularidade da vulnerabilidade em fóruns e comunicações na Darkweb;

26.4.2.8. O mecanismo de priorização deve ser sujeito a modificações e atualizações diárias com base em inteligência de ameaças e observação de tendências na Internet.

26.5. **Da Análise de Risco do Ambiente**

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

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

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

26.5.4. A solução deve ser capaz de realizar um benchmark no ambiente da CONTRATANTE comparando sua maturidade com outras organizações do mesmo setor;

26.5.5. A solução deve prover visão sobre quais ações de remediação reduzem o maior nível de risco do ambiente;

26.5.6. A solução deve também permitir a visualização de ações de remediação agregadas para visão consolidada de redução de risco;

26.5.7. Deve permitir modificar a qualquer momento o tipo de indústria para comparação. Ex: Mudar de Setor Público para Mercado Financeiro;

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

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

26.5.10. A solução deve gerar uma pontuação global referente a exposição cibernética da organização baseado nas pontuações de cada um dos ativos;

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

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

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

26.5.14. A solução deverá apresentar indicadores específicos referentes a remediação, possuindo no mínimo informações referentes ao tempo entre remediação e o tempo o qual a vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades críticas por ativo e a comparação da quantidade de vulnerabilidades corrigidas por criticidade;

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

26.6. Do Gerenciamento da Análise de Ataques exploráveis

26.7. Deve disponibilizar visibilidade nas técnicas de ataque baseado no framework MITRE ATT&CK;

26.7.1. Deve identificar qual a criticidade do ataque, em no mínimo: baixo, médio e alto;

26.7.2. Deve permitir a visualização gráfica dos caminhos de ataque, permitindo uma análise detalhada e intuitiva dos vetores de exploração.

26.7.3. Deve prover a evidência relacionada a descoberta do ataque;

26.7.4. Deve mostrar o objeto relacionado ao ataque, de origem e de destino;

26.7.5. Deve apresentar informações detalhadas relacionadas a mitigação para o ataque em análise;

26.7.6. Deve prover quais ferramentas e possíveis malwares associados ao ataque;

26.7.7. Deve disponibilizar de forma gráfica via console de gerenciamento as conexões entre os objetos do ataque;

26.7.8. Deve disponibilizar uma biblioteca com ‘Queries’ para a busca de objetos no mínimo os seguintes segmentos:

26.7.8.1. Rede;

26.7.8.2. Endpoint;

26.7.8.3. Active Directory;

26.7.8.4. Permissão;

26.7.8.5. Ransomware;

26.7.8.6. Vetores;

26.7.8.7. Credenciamento;

26.7.8.8. Deve suportar no mínimo 90 técnicas de ataques;

26.7.8.9. Deve permitir analisar, ao menos, os seguintes caminhos das superfícies de ataques:

26.7.8.10. Aplicações WEB (DAST);

26.7.8.11. Nuvem;

26.7.8.12. Active Directory;

26.7.8.13. Infraestrutura (Desktops, Servidores).

26.7.9. Deve apresentar os resultados em forma ilustrativa (Dashboard).

26.7.10. O Dashboard deve oferecer uma visão dos seus ativos vulneráveis considerando:

26.7.11. Número de ativos críticos vulneráveis;

26.7.12. Número de caminhos de ataque que levam a esses ativos críticos;

26.7.13. Número de descobertas abertas e sua gravidade;

26.7.14. Matriz para visualizar caminhos com diferentes combinações de valores alvo;

26.7.15. Lista de tendências de caminhos de ataque.

26.7.16. Deve listar as diferenças entre os intervalos de tempo e mostrar uma seta direcional a fim de indicar se o valor aumentou ou diminuiu.

26.7.17. Deve permitir que o caminho de ataque leve a um ativo crítico.

26.7.18. Deve apresentar o número total alcançado de ativos críticos;

26.7.19. Deve apresentar uma tendência dos caminhos de ataque, listando os caminhos de ataques mais populares.

26.7.20. Deve ser possível identificar o host suspeito;

26.7.21. Deve ser possível identificar o usuário suspeito;

26.7.22. Deve ser possível identificar o IP suspeito;

26.7.23. Deve permitir visualização em modo ilustrativo do caminho de ataque;

26.7.24. Deve ser possível identificar qual a técnica utilizada pelo atacante, tais como:

26.7.24.1. Network Sniffing;

26.7.24.2. LSASS Memory;

26.7.24.3. Remote Desktop Protocol;

26.7.24.4. Exploração de serviços remotos;

26.7.24.5. System Services Discovery;

26.7.24.6. Modificação da Política de Grupo;

26.7.24.7. Mecanismo de Controle de Elevação de Abuso.

26.7.25. Deve permitir a comunicação com o framework MITRE ATT&CK ®.

26.7.26. Deve trazer o número de identificação MITRE ATT&CK para a descoberta;

26.7.27. A descoberta no MITRE ATT&CK deve abordar as seguintes ações:

26.7.27.1. A técnica MITRE ATT&CK associada ao achado.

26.7.27.2. A origem da descoberta.

26.7.27.3. O alvo da descoberta.

26.7.27.4. O status para indicar a ação tomada na descoberta, por exemplo, Em andamento.

26.7.28. Deve ser possível exportar uma descoberta como CSV.

26.7.29. Deve ser possível arquivar uma descoberta.

26.7.30. Deve ser possível ver o histórico do log da descoberta.

26.7.31. Deve permitir alterar o status do caminho de ataque descoberto para, pelo menos:

26.7.32. Em Progresso;

26.7.33. Em Revisão;

26.7.34. Feito;

26.8. **Da descoberta de ativos**

26.8.1. A solução deve ser capaz de realizar escaneamento de descoberta de rede utilizando os seguintes critérios como alvo: IP, CIRD e Range;

26.8.2. A solução deve disponibilizar modelos de escaneamento de descoberta, ajustável, com os seguintes tipos de scan:

26.8.2.1. Enumeração de Hosts;

26.8.2.2. Identificação de Sistema Operacional (SO);

26.8.2.3. Port Scan (Portas comuns);

26.8.2.4. Port Scan (Todas as portas);

26.8.2.5. Customizado.

26.8.3. A solução deve permitir realizar escaneamento de descoberta customizado podendo ser parametrizado de acordo com a necessidade.

26.8.4. A parametrização do escaneamento de descoberta deve, no mínimo, conter os seguintes requisitos:

26.8.4.1. Descoberta de Host:

26.8.4.2. Ping o host remoto;

26.8.4.3. Usar descoberta rápida;

26.8.4.4. Métodos de ping:

a) ARP;

b) TCP;

c) ICMP;

d) UDP.

26.8.5. Escaneamento de descoberta de dispositivos de OT;

26.8.6. Escaneamento de descoberta em redes de impressora;

26.8.7. Escaneamento em redes Novell;

26.8.8. Tecnologia de Wake-on-LAN;

26.8.9. Port Scanning:

26.8.10. Portas:

26.8.10.1. Considerar portas não escaneadas como fechadas;

26.8.10.2. Range de portas a serem escaneadas;

26.8.11. Enumerar Portas locais:

26.8.11.1. SSH (netstat);

26.8.11.2. WMI (netstat);

26.8.11.3. SNMP;

26.8.12. Descoberta de Serviços:

26.8.12.1. Sondar todas as portas para encontrar serviços;

26.8.12.2. Procurar por serviços baseado em SSL/TLS;

26.8.12.3. Enumerar todas as cifras SSL/TLS.

26.8.13. A solução deve realizar descoberta de ativo de forma passiva e adicionado automaticamente na console de gerenciamento;

26.8.14. A solução deve descobrir passivamente quando um host é adicionado na rede.

26.9. **Da avaliação de vulnerabilidade**

26.9.1. A solução deve ser capaz de realizar testes sem a necessidade de agentes instalados no dispositivo destino para detecção de vulnerabilidades;

26.9.2. A solução deve detectar e classificar através de severidades, riscos e vulnerabilidades;

26.9.3. A solução deve também fornecer informações detalhadas sobre a natureza da vulnerabilidade, evidências da existência da vulnerabilidade e recomendações para mitigá-los;

26.9.4. A solução deve incluir uma saída detalhada das vulnerabilidades descobertas como versões de DLL esperadas e encontradas;

26.9.5. A solução deve ser compatível com CVE e fornecer pelo menos 10 anos de cobertura CVE;

26.9.6. A solução deve identificar vulnerabilidades especificas para o Active Directory com os seguintes padrões de verificação;

26.9.7. Contas administrativas vulneráveis a Kerberoasting attack;

26.9.8. Utilização de criptografia vulnerável com autenticação Kerberos;

26.9.9. Contas com pré-autenticação do Kerberos desabilitada;

26.9.10. Verificação de usuários com a opção de nunca expirar a senha com a opção habilitada;

26.9.11. Verificar validação de fragilidades do tipo “Unconstrained Delegation”;

26.9.12. Verificação de “Pre-Windows 2000 Compatible Access”;

26.9.13. Verificação de validade de chaves mestras "Kerberos KRBTGT”;

26.9.14. Verificação de “SID History Injection”;

26.9.15. Verificação de “Printer Bug Exploit”;

26.9.16. Verificação de “Primary Group ID”;

26.9.17. Verificação de usuários com Passwords em branco;

26.9.18. A solução deve suportar o uso de SMB e WMI para verificação de sistemas Microsoft Windows;

26.9.19. A solução deve ser capaz de iniciar automaticamente serviços de registro remoto em sistemas Windows ao executar uma varredura credenciada;

26.9.20. A solução deve ser capaz de parar automaticamente o serviço de registro remoto em sistemas Windows novamente assim que a varredura estiver completa;

26.9.21. O scanner deve oferecer suporte a shell seguro (SSH) com a capacidade de escalar privilégios para varredura de vulnerabilidades e auditorias de configuração em sistemas Unix.

26.9.22. A solução deve suportar o uso do netstat (Linux) e WMI (Windows) para uma enumeração rápida e precisa de portas em um sistema quando as credenciais são fornecidas;

26.9.23. A solução deve possibilitar a verificação remota de portas, além da enumeração local de portas, para ajudar a determinar se algum mecanismo de controle de acesso está sendo utilizado;

26.9.24. A solução deve fornecer auditoria de patch (MS Bulletins) para as principais versões de Windows;

26.9.25. A solução deve fornecer auditoria de patch para todos os principais sistemas operacionais Unix incluindo Mac OS, Linux, Solaris e IBM AIX.

26.9.26. A solução deve fornecer varredura para aplicativos comerciais diversos e proprietários, incluindo, mas não limitando-se a: Java, Adobe, Oracle, Apple, Microsoft, Check Point, Palo Alto Networks, Cisco, Fortinet, Fireeye, McAfee, etc.;

26.9.27. A solução deve incluir classificação de severidades de acordo com o padrão Sistema Comum de Pontuação de Vulnerabilidade Versão (CVSS2 e CSVSS 3);

26.9.28. A solução deve fornecer informações acerca da disponibilidade de códigos de exploração das vulnerabilidades encontradas em frameworks de exploração para as plataformas mais populares: Core, Metasploit e Canvas;

26.9.29. A solução deve informar se a vulnerabilidade pode e está sendo ativamente explorada por código malicioso (malware);

26.9.30. A solução deve possuir importação de arquivos;

26.9.31. Deve ser capaz de identificar e classificar vulnerabilidades de máquinas virtuais em nuvem pública em infraestruturas como serviço nas plataformas AWS, Microsoft Azure e Google Cloud.

26.10. Do Inventário de Ativos e mapeamento de exposição

26.10.1. Deve consolidar todos os ativos da organização em uma única interface, incluindo dispositivos, contas de usuário, softwares, ativos em nuvem e aplicações SaaS, facilitando a análise e gestão centralizada.

26.10.2. A solução deve calcular dinamicamente uma pontuação de exposição para cada ativo, variando de 0 a 1000, indicando o nível de risco associado. Pontuações mais altas representarão maior exposição.

26.10.3. Deve atribuir uma classificação de criticidade a cada ativo, em uma escala de 1 a 10, auxiliando na priorização de medidas de segurança com base na importância do ativo para a organização.

26.10.4. Permitir a criação e aplicação de etiquetas (tags), tanto estáticas quanto dinâmicas, para categorizar e organizar ativos conforme critérios específicos, como localização, função ou nível de risco.

26.10.5. As tags devem suportar o agrupamento de ativos on premises. Recursos em núvem, identidades e aplicações Web.

26.10.6. A solução deve oferecer a capacidade de adicionar sinais de exposição personalizados para monitorar combinações específicas de riscos que possam impactar a organização, permitindo uma gestão proativa das fraquezas (vulnerabilidades, configurações incorretas e permissões excessivas).

26.10.7. A plataforma deve permitir a integração com fontes de dados externas e ferramentas de terceiros para uma análise mais aprofundada da exposição e remediação de riscos.

26.10.8. Deve garantir que as informações sobre os ativos sejam atualizadas sempre que um ativo é identificado em uma varredura, mantendo a precisão e relevância dos dados no inventário.

26.10.9. Deve possibilitar a detecção de combinações específicas de vulnerabilidades, exposições de identidade e ameaças que, juntas, aumentam significativamente o risco para a organização.

26.10.10. A plataforma deve possuir uma biblioteca de sinais de exposição pré-definidos pelo fabricante da solução, permitindo às equipes de segurança iniciar rapidamente a identificação de cenários de risco críticos.

26.10.11. A solução deve possibilitar criar sinais de exposição personalizados, utilizando consultas específicas ou processamento de linguagem natural (NLP), adaptando a detecção de riscos às necessidades específicas do negócio.

26.10.12. Deve possibilitar o monitoramento contínuo das violações associadas a cada sinal de exposição, com apresentação de tendências e porcentagens de mudança nos últimos 7 dias, auxiliando na identificação de padrões emergentes.

26.10.13. A plataforma de possuir uma listagem detalhada dos ativos afetados por cada sinal de exposição, incluindo informações como nome do ativo, pontuação de exposição e detalhes específicos das fraquezas identificadas.

26.10.14. Deve possuir funcionalidades para arquivar, editar, duplicar ou excluir sinais de exposição personalizados, proporcionando flexibilidade no gerenciamento dos sinais conforme a evolução das necessidades de segurança.

26.10.15. A solução deve utilizar inteligência artificial para fornecer explicações detalhadas sobre cada sinal de exposição e seus ativos impactados, facilitando a compreensão e a tomada de decisões informadas pelas equipes de segurança.

26.10.16. A plataforma deve unificar as informações de inventário de todos os módulos da solução, com integração nativa ou via API, permitindo uma gestão centralizada e integrada das exposições cibernéticas.

26.11. **Da auditoria de Configuração**

26.11.1. A solução deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino;

26.11.2. A solução deve fornecer benchmarks de auditoria de segurança e configuração para conformidade regulatória e outros padrões de práticas recomendadas pela área ou fabricantes.

26.11.3. A solução deve realizar verificações de auditoria contendo as de segurança, com indicação de sucesso ou falha, baseado nos principais frameworks reconhecidos pela indústria, pelo menos os seguintes:

26.11.3.1. Center for Internet Security Benchmarks (CIS);

26.11.3.2. Defense Information Systems Agency (DISA) STIGs;

26.11.3.3. Health Insurance Portability and Accountability Act (HIPAA);

26.11.3.4. Payment Card Industry Data Security Standards (PCI DSS);

26.11.4. A solução deve fornecer auditoria de programas antivírus para determinação de presença e status de inicialização para no mínimo as seguintes soluções: TrendMicro Office Scan, McAfee VirusScan, Microsoft Endpoint Protection e Kaspersky;

26.11.5. A solução deve fornecer auditorias de configuração com base benchmarks em CIS (Center for Internet Security) L1 e L2, para ambos os sistemas operacionais Microsoft Windows e Linux;

26.11.6. A solução deve permitir auditoria de conformidade em servidores Windows, Linux, Bancos de Dados SQL Server, a fim de determinar se estão configurados de acordo com os principais Framework de segurança como, por exemplo, CIS e DISA;

26.11.7. A solução deve oferecer validação e suporte a SCAP (Security Content Automation Protocol); Solução de análise dinâmica de vulnerabilidades para aplicações Web

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

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

26.11.10. A solução deve avaliar no mínimo os padrões de segurança OWASP Top 10 e PCI (payment card industry data security standard);

26.11.11. A solução deve possuir templates prontos de varreduras entre simples e extensos;

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

26.11.12.1. Cookies, Headers, Formulários e Links;

26.11.12.2. Nomes e valores de parâmetros da aplicação;

26.11.12.3. Elementos JSON e XML;

26.11.12.4. Elementos DOM.

26.11.13. A solução deve permitir somente a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;

26.11.14. A solução deve ser capaz de utilizar scripts customizados de crawl com parâmetros definidos pelo usuário;

26.11.15. A solução deve excluir determinadas URLs da varredura através de expressões regulares;

26.11.16. A solução deve excluir determinados tipos de arquivos através de suas extensões;

26.11.17. A solução deve instituir no mínimo os seguintes limites:

26.11.17.1. Número máximo de URLs para crawl e navegação;

26.11.17.2. Número máximo de diretórios para varreduras;

26.11.17.3. Número máximo de elementos DOM;

26.11.17.4. Tamanho máximo de respostas;

26.11.17.5. Limite de requisições de redirecionamentos;

26.11.17.6. Tempo máximo para a varredura;

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

26.11.17.8. Número máximo de requisições HTTP por segundo;

26.11.18. A solução deve detectar congestionamento de rede e limitar os seguintes aspectos da varredura:

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

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

26.11.19. A solução deve agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;

26.11.20. A solução deve enviar notificações através de no mínimo E-mail e SMS;

26.11.21. A solução deve possuir a flexibilidade de selecionar quais testes serão realizados de forma granular, através da seleção de testes, plug-ins ou ataques;

26.11.22. A solução deve avaliar sistemas web utilizando protocolos HTTP e HTTPs;

26.11.23. A solução deve possibilitar a definição de atributos no cabeçalho (HEADER) da requisição HTTP de forma personalizado a ser enviada durante os testes;

26.11.24. A solução deve ser compatível com avaliação de web services REST e SOAP;

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

26.11.25.1. Autenticação básica (digest);

26.11.25.2. NTLM;

26.11.25.3. Form de login;

26.11.25.4. Autenticação de Cookies;

26.11.25.5. Autenticação através de Selenium;

26.11.26. A solução deve importar scripts de autenticação selenium previamente configurados pelo usuário;

26.11.27. A solução deve customizar parâmetros Selenium como delay de exibição da página, delay de execução de comandos e delay de comandos para recepção de novos comandos;

26.11.28. A solução deve exibir os resultados das varreduras em tendência temporal para acompanhamento de correções e introdução de novas vulnerabilidades;

26.11.29. A solução deve exibir os resultados agregados de acordo com as categorias do OWASP Top 10

26.11.30. (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).

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

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

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

26.11.33.1. Payload injetado;

26.11.33.2. Evidência em forma de resposta da aplicação;

26.11.33.3. Detalhes da requisição HTTP;

26.11.33.4. Detalhes da resposta HTTP;

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

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

26.11.34. A solução deve possuir suporte a varreduras de componentes para no mínimo:

26.11.34.1. Wordpress, Blog Designer Plugin for Wordpress, Event Calendar Plugin for Wordpress, Convert Plus Plugin for Wordpress, AngularJS, Apache, Apache Tomcat, Apache Tomcat JK connecto, Apache Spark e Apache Struts, AtlassianConfluence, Atlassian Crowd e Atlassian Jira, Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Lighttpd, Magento, Modernizr, Nginx, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin e YUI;

26.12. **Solução de análise em imagens de ambientes Containers**

26.12.1. A solução deve ser licenciada contabilizando o número de repositório de imagens únicas, não sendo contabilizada até 10 novas versões de uma mesma imagem em um dia;

26.12.2. A solução deve ser licenciada contabilizando o número de imagens únicas, não sendo contabilizadas novas versões de uma mesma imagem;

26.12.3. A solução deve analisar, testar e reportar falhas de segurança em aplicações em Containers Docker como parte dos ativos a serem inspecionados;

26.12.4. A solução deve ser capaz de analisar imagens preparadas pelos desenvolvedores na esteira DevOps em busca de imagens com vulnerabilidades identificadas e malware residente no sistema de arquivos;

26.12.5. A solução deve integrar a esteira DevOps através de API, invocando o envio da imagem para análise em repositório próprio da solução ou utilizando scanner implementado em infraestrutura proprietária do órgão com a finalidade de evitar o envio de imagens e propriedade intelectual da contratante;

26.12.6. A documentação de API da solução deverá ter acesso público através de website ou documentação do próprio fabricante;

26.12.7. A console de administração deverá possuir controle de acesso no mínimo permitindo usuários com capacidade de somente visualizar as informações, e usuários com capacidade para efetuar análise das imagens;

26.12.8. A solução deve inventariar o sistema operacional de cada imagem analisada e suas vulnerabilidades encontradas;

26.12.9. A solução deve identificar containers que não foram analisados antes de sua implementação em produção;

26.12.10. A solução deve analisar as camadas (layers) de um container;

26.12.11. A solução deve identificar containers que tiveram mudanças de arquivos entre a análise e a sua implementação em produção;

26.12.12. A solução deve informar os CVEs para cada vulnerabilidade encontrada nos pacotes e bibliotecas residentes na imagem;

26.12.13. A solução deve ter a capacidade de testar automaticamente todas as imagens armazenadas, ou previamente testadas, sempre que uma nova vulnerabilidade for publicada e atualizada no banco de dados de vulnerabilidade da solução, sem qualquer tipo intervenção manual;

26.12.14. A solução deve inventariar os pacotes e bibliotecas e suas respectivas versões e listar as mesmas dentro do relatório de resultados de análise de cada imagem;

26.12.15. A solução deve possuir conectores e permitir importação de imagens dos seguintes repositórios:

26.12.15.1. Docker;

26.12.15.2. Docker EE;

26.12.15.3. AWS ECR;

26.12.15.4. JFrog Artifactory.

26.12.16. A solução deve possuir integração com Microsoft Azure Container, Vmware Harbor e Sonatype Nexus para importar e analisar imagens;

26.12.17. A solução deve fornecer scanner em formato Docker para implementação local e análise de imagens sem a necessidade de envio destas para repositório remoto, fora do ambiente da contratante;

26.12.18. A solução ser capaz de configurar políticas usando como condições: CVSS Score, CVEs específicos e Malware identificado;

26.12.19. A solução deve permitir a criação de políticas específicas por repositório;

26.12.20. A solução deve prover integração com as seguintes plataformas de integração contínua: Azure Pipeline, Jenkins, Github Actions e GitLab;

26.12.21. Solução de análise de código em ambiente DevOps;

26.12.22. A solução deve detectar e configurações incorretas da infraestrutura de nuvem em fases de design, construção e tempo de execução do seu ciclo de vida de desenvolvimento de software;

26.12.23. A solução deve prevenir problemas de segurança identifique e remova falhas na nuvem durante desenvolvimento antes de chegarem à produção;

26.12.24. A solução deve ser possível avaliar modelos de infraestrutura como código (IaC), com integrações em:

26.12.24.1. Terraform;

26.12.24.2. AWS CloudFormation;

26.12.24.3. Azure Resource Manager;

26.12.24.4. Kubernetes.

26.12.25. A solução deve prevenir o desvio de postura na nuvem identifique discrepâncias entre o IaC e sua nuvem em execução ambiente;

26.12.26. A solução deve fornecer sugestões de correção automaticamente por meio de pull ou mesclagem;

26.12.27. A solução deve contextualizar riscos compreender as vulnerabilidades de aplicativos no contexto de suas configurações de infraestrutura para obter uma imagem real do risco que eles presente;

26.12.28. A solução deve prover integração no mínimo com as seguintes plataformas abaixo:

26.12.28.1. Jira;

26.12.28.2. Slack;

26.12.28.3. AWS SNS;

26.12.28.4. Jenkins;

26.12.28.5. Terraform Cloud;

26.12.28.6. CircleCI;

26.12.28.7. Splunk;

26.12.28.8. AWS CloudTrail.

26.12.29. A solução deve possuir integração com no mínimo os seguintes Repositórios:

26.12.29.1. Bitbucket;

26.12.29.2. GitHub;

26.12.29.3. GitLab;

26.12.29.4. Azure DevOps.

26.12.30. A solução deve possuir funcionalidade de monitoramento dos repositórios sempre que houver alteração de código uma verificação automática via IaC deve apresentar a diferença;

26.12.31. A solução deve possuir políticas de análise em ambiente de nuvem para no mínimo as seguintes plataformas:

26.12.31.1. AWS;

26.12.31.2. Azure;

26.12.31.3. GCP;

26.12.31.4. Kubernetes.

26.12.32. A solução deve possuir análise por benchmarks e compliance para os seguintes padrões em formato de Dashboard:

26.12.32.1. CIS;

26.12.32.2. NIST;

26.12.32.3. ISO-27001;

26.12.32.4. HIPAA;

26.12.32.5. PCI-DSS;

26.12.32.6. CCM;

26.12.32.7. GDPR;

26.12.32.8. LGPD.

27. **SOLUÇÃO DE GERENCIAMENTO DE VULNERABILIDADES E VISIBILIDADE DE ATAQUES EM TEMPO REAL PARA ESTRUTURA DE DIRETÓRIO DE USUÁRIOS, COM ANÁLISE CONTÍNUA E ADAPTÁVEL DE RISCOS E CONFIANÇA (ITEM 6)**

27.1. **Solução de análise em ambiente Microsoft Active Directory**

27.1.1. A solução deve identificar fraquezas ocultas em configurações do dedicadas ao Active Directory;

27.1.2. A solução deve possuir ações preventivas de hardening para o Active Directory;

27.1.3. A solução deve identificar ataque específicos para a estrutura do Active Directory;

27.1.4. A solução deve possuir funcionalidade para analisar em detalhes cada configuração incorreta que acarreta riscos de segurança – com uma linguagem simples, contextualizando tal risco para os times envolvidos;

27.1.5. A solução deve possuir recomendações de correção para cada configuração incorreta no Active Directory;

27.1.6. A solução deve avaliar relações de confiança perigosas entre florestas e domínios;

27.1.7. A solução deve capturar as mudanças que ocorrem no AD e demonstrar na console de administração;

27.1.8. A solução deve possuir dashboard com os principais ataques e vulnerabilidades por domínio;

27.1.9. A solução deve permitir a correlação de mudanças no Active Directory e desvios de segurança;

27.1.10. A solução deve analisar em detalhes um ataque explorando as descrições através do framework MITRE ATT&CK;

27.1.11. A solução deve prover interface web para gerenciamento de todas as funcionalidades;

27.1.12. A solução deve possuir capacidade nativa de criação de dashboards customizados;

27.1.13. A solução deve suportar um modelo de controle de acesso baseado em funções (RBAC) flexível;

27.1.14. A solução deve demonstrar alterações no Active Directory, seus objetos e atributos;

27.1.15. A solução deve armazenar ou sincronizar nenhuma credencial de objetos do Active Directory;

27.1.16. A solução deve suportar ambientes com múltiplas florestas e domínios;

27.1.17. A solução deve suportar monitoramento contínuo de ambientes com Active Directory com o nível funcional de floresta e domínio a partir do 2003;

27.1.18. A solução deve suportar reter os eventos coletados por no mínimo um ano;

27.1.19. A solução deve descobrir e mapear a superfície de ataque do Active Directory e seus domínios monitorados com os seguintes padrões:

27.1.20. Não depender de agentes para coleta de informações no AD;

27.1.21. A solução deve seguir as boas práticas de menor privilégio, a conta de serviço utilizada para conexão com o Active Directory, sendo o menor nível de acesso esperado para a conta de serviço como parte do grupo Domain User;

27.1.22. Interface web que consolida e apresenta de maneira unificada os domínios monitorados e as possíveis relações de confiança estabelecidas entre eles;

27.1.23. A solução deve analisar continuamente a postura de segurança do AD, minimamente avaliando:

27.1.24. Validação de GPOs desvinculadas, desabilitadas ou órfãs;

27.1.25. Validação de contas desativadas em grupos privilegiados;

27.1.26. Domínio usando uma configuração perigosa de compatibilidade com versões anteriores por meio de alterações no atributo dSHeuristics;

27.1.27. Validação de atributos relacionados a roaming de credenciais vulneráveis (ms-PKI-DPAPIMasterKeys) gerenciados por um usuário sem privilégios;

27.1.28. Validação de domínio sem GPOs de proteção de computador, desativando protocolos vulneráveis antigos, como NTLMv1;

27.1.29. Validação de contas com senhas que nunca expiram;

27.1.30. Validação de senhas reversíveis em GPOs;

27.1.31. Validação de uso de senhas reversíveis em contas de usuário;

27.1.32. Validação de utilização de protocolo criptográfico fraco (Ex. DES) em contas de usuário;

27.1.33. Validação de uso do LAPS (Solução de senha de administrador local) para gerenciar senhas de contas locais com privilégios;

27.1.34. Validação se o domínio possui um nível funcional desatualizado;

27.1.35. Validação de contas de usuário utilizando senha antiga;

27.1.36. Validação se o atributo AdminCount está definido em usuários padrão;

27.1.37. Validação do uso recente da conta de administrador padrão;

27.1.38. Validação de usuários com permissão para ingressar computadores no domínio;

27.1.39. Validação de contas dormentes;

27.1.40. Validação de computadores executando um sistema operacional obsoleto;

27.1.41. Validação de restrições de logon para usuários privilegiados em ambiente com múltiplos tiers (1, 2 e 3) de segregação de ativos;

27.1.42. Validação de direitos perigosos configurados no Schema do AD;

27.1.43. Validação de relação de confiança perigosa com outras Florestas e Domínios;

27.1.44. Validação de contas que possuem um atributo perigoso de histórico SID (SID History);

27.1.45. Validação de contas utilizando controle de acesso compatível com versões anteriores ao Windows 2000;

27.1.46. Validação da última alteração de senha do KDC;

27.1.47. Validação da última alteração da senha da conta SSO do Azure AD;

27.1.48. Validação de contas que podem ter senha em branco/vazia;

27.1.49. Validação de utilização do grupo nativo Protected Users;

27.1.50. Validação de privilégios sensíveis (Ex. Debug a program, Replace a process level token, etc.) perigosos atribuídos aos usuários;

27.1.51. Validação de possível senha em clear-text;

27.1.52. Validação de sanidade das GPOs e componentes CSEs (Client-Side Extension);

27.1.53. Validação de uso de algoritmos de criptografia fracos na PKI do Active Directory;

27.1.54. Validação de contas de serviço com SPN (Service Principal Name) que fazem parte de grupos privilegiados;

27.1.55. Validação de contas anormais nos grupos administrativos padrão do AD;

27.1.56. Validação de consistência no container adminSDHolder;

27.1.57. Validação de delegação Kerberos perigosa;

27.1.58. Validação em permissões de objetos raiz que permitem ataques do tipo DCSync;

27.1.59. Validação de políticas de senha fracas aplicadas aos usuários;

27.1.60. Validação das permissões relacionadas às contas do Azure AD Connect;

27.1.61. Validação do ID do grupo primário do usuário (Primary Group ID);

27.1.62. Validação de permissões em GPOs sensíveis associadas aos Containers Configuration, Sites, Root Partition e Ous sensíveis como Domain Controllers;

27.1.63. Controladores de domínio gerenciados por usuários ilegítimos;

27.1.64. Validação de certificado mapeado através de atributo altSecurityIdentities em contas privilegiadas;

27.1.65. Validação de uso de protocolo Netlogon inseguro (Zerologon/CVE-2020-1472);

27.1.66. A solução deve identificar vulnerabilidades e configurações incorretas do AD à medida que são introduzidas sendo:

27.1.67. Identificar todas as vulnerabilidades e configurações incorretas no AD;

27.1.68. Monitorar relações de confiança perigosas em toda a estrutura AD;

27.1.69. Apresentar ameaças e alterações sem a necessidade de scans estáticos e programados no Active Directory e sua infraestrutura;

27.1.70. Apresentar as ameaças e alterações em tempo real;

27.2. **Detecção e resposta a ataques:**

27.2.1. Monitorar continuamente os indicadores de possíveis ataque como DCSync, DCShadow, Password Spraying, Password Guessing/Brute Force, Lsaas Injecton nos controladores de domínio, Golden Ticket, NTLM Relay, entre outros;

27.2.2. Detecção de ataques ao AD em tempo real;

27.2.3. Análise detalhada do ataque, apresentando ativo de origem, vetor de ataque, controlador de domínio afetado, técnica aplicada;

27.2.4. Apresentação de ataques em uma linha do tempo;

27.2.5. Investigar ameaças, reproduzir ataques e procurar por backdoors;

27.2.6. Permitir busca ágil de eventos específicos na base da solução através de queries customizadas;

27.2.7. A solução deve ser capaz de enviar alertas por e-mail;

27.2.8. A solução nativamente deve ser capaz de se integrar com SIEM através de protocolo SYSLOG;

27.2.9. A solução deve ser capaz de filtrar e enriquecer os eventos que serão enviados para o SIEM;

27.2.10. A solução deve produzir regras YARA na detecção de ataques (Ex. DCSync, Golden Ticket) identificados pela ferramenta;

27.2.11. A solução deve possuir conjunto de APIs REST, todas as chamadas disponíveis devem estar contidas na documentação;

27.2.12. A solução deve permitir a criação de listas de exclusões, suportando minimamente Exclusão por domínios do AD monitorados e por itens analisados;

27.2.13. A solução deve ser licenciada pelo número de usuários habilitados;

28. **SERVIÇO DE SUPORTE PROATIVO, CORRETIVO E PARA RESPOSTA A INCIDENTES (ITEM 7)**

28.1. O serviço de suporte proativo, corretivo e para resposta a incidentes compreende um conjunto abrangente de atividades destinadas a assegurar o pleno funcionamento e a continuidade operacional de sistemas, soluções ou serviços. Este serviço é estrategicamente desenhado para atender às demandas dinâmicas do ambiente tecnológico, oferecendo suporte preventivo, corretivo e uma resposta ágil a incidentes de segurança.

28.2. Todo o Serviço de Suporte deverá ser prestado por profissional certificado pelo Fabricante da Solução, em nível compatível com a prestação do serviço. Deverá ser apresentada comprovação da certificação dos profissionais responsáveis no ato da assinatura do contrato.

28.3. Deverá disponibilizar um serviço preventivo de verificação e atualização de versões ou correções (patches) que se fizerem necessários, específicos para a solução ofertada;

28.4. deverá prestar suporte a todos os componentes de software fornecidos que forem necessários para a implementação e utilização da solução.

28.5. **Suporte Proativo:**

28.5.1. O suporte proativo deverá antecipar potenciais problemas, identificando e resolvendo questões antes mesmo que impactem o desempenho e a segurança do ambiente;

28.5.2. A contratada deverá notificar a contratante sobre atualizações de segurança, patches e correções assim que estiverem disponíveis, caso autorizado aplicar as atualizações de segurança e evolutiva dos produtos;

28.5.3. Deverá realizar análises preditivas, buscando otimizar a performance e prevenir falhas nos produtos, além de detectar padrões que possam indicar uma possível violação de segurança, proporcionando um ambiente mais estável e seguro;

28.5.4. Deverá realizar avaliações regulares de riscos para identificar possíveis vulnerabilidades e pontos fracos nos sistemas e, implementar medidas corretivas com base nos resultados das avaliações de riscos;

28.5.5. Realizar auditorias regulares para garantir que as melhores práticas e os controles de segurança estejam operacionais e, utilizar resultados de auditorias para implementar melhorias contínuas;

28.5.6. A CONTRATADA deverá apresentar relatório contendo as ações adotadas para a solução do problema.

28.6. **Suporte Corretivo:**

28.6.1. Este componente concentra-se na solução de problemas ou incidentes. O suporte corretivo atua de forma ágil para restabelecer a funcionalidade normal do sistema, minimizando impactos negativos e mantendo a continuidade operacional;

28.6.2. Serviço Especializado de Suportes corretivo para 24 meses. Serviço de Suporte especializado para ajustes, correções e configurações da solução a ser fornecida. Neste serviço deverá estar incluso todo tipo de suporte para funcionamento da solução;

28.6.3. A contratada deverá:

- Implementar um sistema de abertura de chamados, para registrar, rastrear e priorizar incidentes e requisições de suporte;
- Atribuir números de caso exclusivos para facilitar a comunicação e o acompanhamento;

- Garantir disponibilidade 24/7 para responder a incidentes críticos.

28.6.4. Deverá apresentar relatório contendo as ações adotadas para a solução do problema.

28.7. **Resposta a Incidentes:**

28.7.1. O serviço de resposta a incidentes deverá lidar com eventos imprevistos, como violações de segurança, falhas críticas ou interrupções inesperadas. deverá ser realizada por profissionais especializados e certificados pelo fabricante;

28.7.2. Deverá realizar investigações para determinar a natureza, origem e impacto de incidentes de segurança;

28.7.3. Desenvolver planos de mitigação e estratégia de recuperação para minimizar o impacto de incidentes;

28.7.4. Elaborar relatórios detalhados sobre os incidentes, incluindo ações tomadas e recomendações de melhorias.

29. **SERVIÇO DE IMPLANTAÇÃO (ITEM 8)**

29.1. Nesta etapa, compreende-se a instalação e configuração da solução contratada, contados a partir da emissão da Ordem de Serviço (OS);

29.2. O serviço de implantação abrange integralmente as fases essenciais para a integração, instalação e configuração da solução contratada, alinhando-se precisamente com as especificações técnicas e requisitos predefinidos. Esta abordagem abarca desde o planejamento inicial até a conclusão efetiva, assegurando uma transição suave dos processos existentes para a nova solução;

29.3. O Plano de Implantação assume a forma de um documento fundamental que consolida a estratégia para instalação, configuração e entrega da solução contratada. Sua importância reside em orientar e alinhar as atividades, garantindo eficiência e uma implementação adequada da solução conforme os requisitos estabelecidos;

29.4. O documento deverá conter no mínimo os requisitos de ambiente tecnológicos necessários para a instalação das licenças, cronograma e detalhamento das atividades a serem realizadas, topologia do ambiente pós instalação da solução, matriz de responsabilidade, plano de comunicação;

29.5. Durante esta etapa, a equipe da Contratada deverá estar presente nos horários de instalação definidos pelo Contratante. As atividades de instalação e configuração poderão ser realizadas, conforme necessário, em horário comercial, período noturno ou final de semana;

29.6. O Contratante disponibilizará a infraestrutura de hardware e software necessária e já existente em seu ambiente, incluindo o ambiente virtualizado, sistema operacional, banco de dados, e outros, para a instalação e configuração da solução durante esta etapa.

30. **SERVIÇO DE CAPACITAÇÃO E REPASSE DE CONHECIMENTO (ITEM 9)**

30.1. Repasse de conhecimento, na forma de treinamento para técnicos, de forma virtual, para 1 (uma) turma, com carga horária mínima de 40 (quarenta) horas, abrangendo todos os softwares integrantes da suíte de solução de segurança;

30.2. O conteúdo programático abordará tanto aspectos teóricos quanto práticos, contemplando de maneira abrangente todos os módulos relevantes da solução de segurança;

30.3. O treinamento pode ser segmentado de acordo com o produto a ser instalado no ambiente tecnológico, contemplando, no mínimo, os seguintes módulos:

30.3.1. Instalação do módulo de gerenciamento central;

30.3.2. Instalação do software de Endpoint Protection em estações de trabalho e servidores;

30.3.3. Descrição e configuração de todas as funcionalidades contratadas da solução;

30.3.4. Melhores práticas utilizadas no mercado para otimização dos softwares e suas funcionalidades.

30.4. A carga horária mínima estabelecida será de 40 (quarenta) horas, divididas em expedientes de 4 horas por dia, no horário comercial. A contratada é responsável por fornecer apostilas em formato digital que contemplem o conteúdo referente ao produto, oferecendo suporte ao aprendizado prático e teórico dos participantes;

30.5. Este treinamento visa capacitar adequadamente os usuários finais, garantindo que compreendam e aproveitem plenamente as funcionalidades da solução de segurança. O enfoque prático e teórico, aliado às melhores práticas do mercado, promove uma formação abrangente e eficaz.

31. **SERVIÇO DE MONITORAMENTO DO AMBIENTE PRESENCIAL (ITEM 10)**

31.1. O serviço de monitoramento do ambiente tecnológico presencial consiste em um conjunto de práticas e procedimentos voltados para a supervisão constante e vigilância dos recursos e sistemas tecnológicos em um determinado espaço físico. Esse serviço é essencial para garantir a segurança, integridade e o desempenho eficiente da infraestrutura tecnológica.

31.2. Principais Componentes do Serviço:

31.2.1. Monitoramento em tempo real, visando a identificação proativa de ameaças e eventos de segurança e garantir o correto funcionamento dos produtos;

31.2.2. Relatórios periódicos, incluindo métricas de desempenho, incidentes de segurança identificados e ações tomadas;

31.2.3. Disponibilidade Contínua: Garantir o funcionamento ininterrupto dos serviços de segurança;

31.2.4. Prevenção de Falhas: Identificar antecipadamente possíveis falhas ou problemas, permitindo a intervenção antes que impactem a operação;

31.2.5. Segurança de Dados: Assegura a integridade e confidencialidade dos dados armazenados e processados no ambiente tecnológico;

31.2.6. Eficiência Operacional: Contribui para a otimização do desempenho dos equipamentos e a eficácia nas operações;

31.2.7. Conformidade e Auditoria: Facilita o cumprimento de normas regulatórias e possibilita auditorias internas e externas.

31.3. O serviço de monitoramento do ambiente tecnológico presencial é essencial para garantir a segurança, eficiência e disponibilidade dos recursos tecnológicos em um local físico, sendo uma parte fundamental da gestão proativa da infraestrutura tecnológica de uma organização.

Documento assinado eletronicamente por **UBALDO DE SÁ NEVES JÚNIOR - Matr.372815-3**, **Diretor**, em 30/06/2025, às 12:20, conforme horário oficial de Brasília, com fundamento no Cap. III, Art. 14 do Decreto Estadual nº 18.142, de 28 de fevereiro de 2019.

A autenticidade deste documento pode ser conferida no site https://sei.pi.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **018258703** e o código CRC **50160A37**.

Referência: Processo nº 00002.012947/2023-48 SEI nº 018258703