Rio PREFEITURA | CASA CIVIL | IPLANRIO

TERMO DE REFERÊNCIA

REGISTRO DE PREÇOS PARA EXPANSÃO DA SOLUÇÃO TRENDMICRO PARA PROTEÇÃO DE SERVIDORES, INCLUINDO PROTEÇÃO DE CONTAINERS E NUVEM, VISIBILIDADE DE REDE, MÓDULO DE DETECÇÃO E RESPOSTA MULTICAMADAS DE AMEAÇAS, GARANTIA TÉCNICA DE 24 (VINTE E QUATRO) MESES E ALOCAÇÃO DE TÉCNICO RESIDENTE

julho / 2025

1 DO OBJETO

1.1. Registro de Preços para Expansão da solução de segurança Trendmicro para proteção de servidores, incluindo a solução proteção de containers e nuvem, solução de visibilidade de redes e módulo de detecção e resposta multicamadas de ameaças, com garantia técnica de 24 (vinte e quatro) meses e alocação de técnico residente, conforme descrito e caracterizado neste Termo de Referência.

1.2. O objeto descrito neste Termo de Referência é caracterizado como comum, tendo em vista que foi objetivamente definido neste documento por meio de especificações usuais do mercado.

1.3. Trata-se de objeto disponível em mercado próprio, fornecido habitualmente, independentemente da demanda da Administração, de forma padronizada, sem a exigência de atendimento a qualquer especificidade ou variantes de adequação.

1.4. O objeto do presente processo licitatório foi dividido em 3 (três) itens.

2 DA JUSTIFICATIVA DA NECESSIDADE DA CONTRATAÇÃO.

A) Item 1

Considerando a relevância estratégica e a criticidade da segurança cibernética para garantir a continuidade operacional da solução tecnológica já pré-existente, atendendo ao princípio da padronização, torna-se imprescindível a realização da presente contratação para a continuidade da integridade das informações e conformidade normativa da PCRJ. Além disso, diante de tais aspectos, faz-se necessária a expansão da atual solução tecnológica para que haja a plena proteção de servidores já implantada e em operação.

Diante disto, a solução tecnológica para proteção de servidores da TRENDMICRO foi previamente selecionada, contratada e implantada após rigorosa análise por intermédio de critérios técnicos e econômicos, evidenciando a compatibilidade técnica integral, desempenho satisfatório e comprovada eficácia na proteção contra ameaças digitais. A expansão com tecnologia de marca e modelo idênticos é essencial, pois garante:

- Compatibilidade Técnica: permite integração nativa e plena interoperabilidade com a infraestrutura tecnológica atual, evitando riscos operacionais decorrentes de incompatibilidades técnicas ou falhas sistêmicas.

- Padronização Tecnológica: atende ao disposto na alínea a) do inc. I do Art. 4723 da Lei nº 13/303/2016 e ainda, na alínea a) do inc. I do Art. 62 do Regulamento de Licitações e Contratos do IPLANRIO, que autoriza padronização técnica devidamente fundamentada em critérios objetivos, para assegurar eficiência na manutenção, operação e treinamento dos servidores públicos envolvidos na gestão da solução tecnológica.

- Redução de custos operacionais e de treinamento: utilizar tecnologia já conhecida pela equipe reduz significativamente custos adicionais relacionados a treinamentos técnicos, bem como os custos operacionais e administrativos resultantes da gestão de múltiplos sistemas distintos.

- Continuidade e Confiabilidade: a expansão com solução idêntica fortalece a segurança e garante continuidade operacional, visto que a integração direta evita vulnerabilidades que poderiam surgir com soluções não compatíveis.

Assim, com fundamento na alínea a) do inc. I do o Art. 4723 da Lei nº 13/303/2016, 14.133/2021 e ainda, na alínea a) do inc. I do Art. 62 do Regulamento de Licitações e Contratos do IPLANRIO, justifica-se tecnicamente a necessidade de licitação específica para aquisição de expansão da solução de proteção de servidores da TRENDMICRO, visando assegurar a continuidade operacional, a integridade dos dados e a eficiência administrativa.

Por fim, estamos diante de contratação atual que visa a expansão de itens já contratados anteriormente, tornando-se necessária a observância da padronização para aquisição de determinado produto ou contratação de serviços. As características técnicas e condições de manutenção, assistência técnica e garantia são técnica e economicamente mais vantajosas, diante da necessidade e conveniência de continuidade do objeto já anteriormente contratado

B) Item 2

Considerando o aumento da adoção de contêineres e tecnologias de nuvem pela PCRJ para a disponibilização de serviços essenciais à população, atualmente, estes não contam com cobertura de solução tecnológica contra contra-ataques cibernéticos para este ambiente, faz-se necessária a aquisição de solução especializada para proteção deste ambiente crítico e estratégico.

De acordo com os fatos acima mencionados, a solução de proteção de containers e ambientes virtualizados da TrendMicro é imprescindível devido aos seguintes aspectos:

- Compatibilidade e Integração Técnica: permite que haja a integração plena com as soluções já devidamente implantadas de proteção de servidores e

endpoints em contratação anterior, garantindo uma defesa homogênea e eficaz em todos os níveis de infraestrutura digital.

- Proteção Específica para Containers: assegura proteção eficaz para ambientes virtualizados e containers, prevenindo ameaças específicas comuns nesses ambientes, tais como vulnerabilidades em aplicações e ataques direcionados.

- Padronização Tecnológica: atende ao disposto na alínea a) do inc. I do Art. 47 da Lei nº 13/303/2016 e ainda, na alínea a) do inc. I do Art. 62 do Regulamento de Licitações e Contratos do IPLANRIO, que autoriza padronização técnica devidamente fundamentada em critérios objetivos, para assegurar eficiência na manutenção, operação e treinamento dos servidores públicos envolvidos na gestão da solução tecnológica.

Diante disso, com respaldo nos artigos 23 e 41 da Lei nº 14.133/2021, fica plenamente justificada a aquisição específica da solução de proteção para ambientes de containers e virtualizados da TrendMicro, visando assegurar maior eficácia operacional, segurança tecnológica e compliance regulatório.

C) Item 3

Considerando a necessidade crítica de uma visão abrangente e proativa sobre o ambiente computacional da PCRJ para detectar, mitigar e responder rapidamente às ameaças cibernéticas em sua extensa camada de rede, justifica-se a aquisição da solução de visibilidade de rede da TrendMicro, fundamentada nos seguintes aspectos:

- Compatibilidade e Integração Técnica: permite que haja a integração plena com as soluções já devidamente implantadas de proteção de servidores e endpoints em contratação anterior, garantindo uma defesa homogênea e eficaz em todos os níveis de infraestrutura digital.

- Visibilidade Aprimorada: permite monitorar e analisar integralmente o tráfego de rede e comportamento dos usuários, proporcionando a identificação precoce e precisa de ameaças e atividades suspeitas.

- Detecção e Resposta Multicamadas: fornece capacidades avançadas de detecção e mitigação em diversos níveis, contribuindo diretamente para a redução do impacto das ameaças e rápida recuperação de incidentes.

- Compatibilidade e Integração: assegura integração perfeita com a infraestrutura existente, especialmente com a solução de proteção de servidores e endpoints, otimizando a comunicação entre módulos, facilitando a gestão centralizada e reduzindo significativamente a complexidade operacional.

- Redução de custos e Complexidade Operacional: a aquisição integrada facilita significativamente a gestão centralizada, reduz custos operacionais adicionais e minimiza complexidades técnicas e administrativas.

- Fornecimento de Serviços Técnicos Especializados: para garantir eficiência, desempenho e segurança na implantação e operação, faz-se necessário que o mesmo fornecedor preste serviços técnicos especializados de instalação, configuração e suporte contínuo, conforme previsto na legislação vigente.

Dessa forma, com respaldo na alínea a) do inc. I do o Art. 4723 da Lei nº 13/303/201614.133/2021 e ainda, na alínea a) do inc. I do Art. 62 do Regulamento de Licitações e Contratos do IPLANRIO, fica plenamente justificada a aquisição específica da solução de visibilidade de rede da TrendMicro, incluindo suporte técnico especializado para implementação, configuração e operação contínua, essencial para ambientes críticos que exigem alta disponibilidade e resposta imediata a incidentes.

3 CARACTERÍSTICAS GERAIS DA SOLUÇÃO

3.1. DESCRIÇÃO DA SOLUÇÃO E DOS SERVIÇOS

Item 1	Descrição da Solução	Tipo	Qtde
1	Solução de Segurança TRENDMICRO para proteção de servidores com módulo de detecção e resposta a ameaças avançadas, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses. (item 3.2 deste Termo de Referência)	Subscrição	1.000

Item 2	Descrição da Solução	Tipo	Qtde
2	Solução de Segurança TRENDMICRO para Containers e Nuvem com módulo de detecção e resposta a ameaças avançadas, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses. (item 3.3 deste Termo de Referência)	Subscrição	19

Item 3	Descrição da Solução	Tipo	Qtde
3.1	Solução de Visibilidade de Rede TRENDMICRO composta de equipamento físico para visibilidade de rede e funcionalidade de monitoramento de rede com módulo de detecção e resposta a ameaças avançadas, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses. (item 3.4 deste Termo de Referência)	Und	01

3.2	Serviços de Instalação, configuração da Solução Visibilidade de Rede.	Serviço	01
3.3	Serviço de Técnico Residente por 24 meses (item não dependente dos itens 3.1 e 3.2)	Serviço	01

3.2. **SOLUÇÃO DE SEGURANÇA TRENDMICRO PARA PROTEÇÃO DE SERVIDORES COM MÓDULO DE DETECÇÃO E RESPOSTA A AMEAÇAS AVANÇADAS, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 24 (VINTE E QUATRO) MESES.**

3.2.1. A solução de proteção de servidores e cargas de trabalho em nuvem deverá possuir integração com a plataforma de resposta à incidentes existente no ambiente.

3.2.2. O gerenciamento da solução deverá ser realizado de forma centralizada pela plataforma de resposta à incidentes.

3.2.3. Deve ser permitido através da plataforma de resposta à incidentes a criação de diversos perfis e usuários para acesso a console de administração da camada de proteção para servidores e cargas de trabalho em nuvem.

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

3.2.4.1. Windows Server 2016;

3.2.4.2. Windows Server 2019;

3.2.4.3. Windows Server 2022;

3.2.4.4. Red Hat Enterprise 6, 7, 8 e 9;

3.2.4.5. SUSE Linux Enterprise Server 12 e 15;

3.2.4.6. CentOS 6, 7 e 8;

3.2.4.7. Cloud Linux 7 e 8;

3.2.4.8. Oracle Linux 6, 7, 8 e 9;

3.2.4.9. Ubuntu 16, 18, 20, 22 e 24;

3.2.4.10. Debian 9,10,11,12;

3.2.4.11. AlmaLinux 8 e 9;

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

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

3.2.7. Deverá ser compatível com servidores físicos, virtuais e em nuvem.

3.2.8. 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.

3.2.9. 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, Puppet e Novel Zen Works;

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

3.2.11. Todos os eventos e ações realizadas na console de gerenciamento precisam ser gravados, visando a auditoria;

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

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

3.2.14. A solução deverá permitir que a distribuição de vacinas e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente, diminuindo o tráfego de internet;

3.2.15. 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;

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

3.2.17. A solução deverá fornecer pelo menos relatórios em dois dos seguintes formatos PDF, CSV, XLS e RTF;

3.2.18. A solução deve permitir que relatórios no formato PDF, possam ser enviados com proteção de uma senha única para cada destinatário;

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

3.2.20. Como a solução ofertada é em nuvem, o ambiente do fabricante deverá fornecer alta disponibilidade;

3.2.21. Os usuários devem ter privilégios para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial";

3.2.22. 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;

3.2.23. Toda comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;

3.2.24. Cada agente deverá ter sua própria chave para criptografia a fim de garantir que a comunicação criptografada seja feita de forma diferente para cada agente instalado;

3.2.25. A console de gerenciamento deverá possuir dashboards para facilitar a monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;

3.2.26. 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 podendo ser automatizados através de script PowerShell;

3.2.27. 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 podendo ser automatizados através de bash script;

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

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

3.2.30. Deve permitir a remoção automática de agentes inativos, com a possibilidade de definir o período;

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

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

3.2.33. A solução deverá dispor de perfis pré-definidos e aptos a funcionarem de acordo com sua denominação;

3.2.34. A solução deverá mostrar de forma simples quais máquinas estão usando determinada política;

3.2.35. Os agentes deverão ter a capacidade de executar rastreamento nas máquinas onde estão instalados e fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;

3.2.36. Esses rastreamentos devem ocorrer de forma agendada a ser definida pelo administrador;

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

3.2.38. 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;

3.2.39. 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;

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

3.2.41. 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;

3.2.42. 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;

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

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

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

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

3.2.47. Após as atualizações devem ser informados o que foi modificado ou adicionado;

3.2.48. Deve ser possível baixar as assinaturas na console de gerenciamento, com opção de não distribuí-las aos clientes;

3.2.49. A console de gerenciamento deve apresentar a capacidade de gerar rollback de suas atualizações de regras;

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

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

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

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

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

3.2.55. 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;

3.2.56. O fabricante da solução deve possuir programa de pesquisa em vulnerabilidades;

3.2.57. A solução deve possuir API documentada para integração em esteira de automação;

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

3.2.59. Deve 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;

3.2.60. A solução deve permitir desabilitar os módulos individualmente;

3.2.61. Deve 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.

3.2.62. A solução deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e agendamento, com possibilidade de tomada de ações distintas para cada tipo de ameaça;

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

3.2.64. 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;

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

3.2.66. 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;

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

3.2.68. O scan de arquivos comprimidos do tipo OLE deverá ser de no mínimo 8 camadas de compressão;

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

3.2.70. A solução deverá possuir a funcionalidade de monitoramento de comportamento para detectar mudanças e atividades suspeitas não autorizadas;

3.2.71. A solução deverá oferecer a opção de escanear processos em memória em busca de Malware;

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

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

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

3.2.75. A solução deverá mostrar informação da data sobre o último scan agendado ou manual executado;

3.2.76. Possuir a capacidade de efetuar backup e restaurar arquivos comprometidos por Ransomware;

3.2.77. Deve possuir cache dos arquivos verificados de modo a evitar redundância da varredura;

3.2.78. Deve possibilitar o controle do consumo de memória durante as varreduras a fim de minimizar os impactos de desempenho nos servidores;

3.2.79. A solução deve possuir opção para forçar a comunicação com o agente e coletar os respectivos logs;

3.2.80. Em servidores Windows, deve possuir capacidade de detectar ameaças por comportamento;

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

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

3.2.83. 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;

3.2.84. A solução deve permitir alterar o nível de sensibilidade para detecção de URLs maliciosas;

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

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

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

3.2.88. A solução deve permitir que o administrador reclassifique uma URL através do site do fabricante a fim de evitar falsos positivos;

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

3.2.90. Deve operar como firewall de host, através da instalação de agente nos servidores protegidos. Não serão aceitas soluções que administrem firewalls terceiros;

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

3.2.92. Deve ter a capacidade de controlar conexões TCP baseado nas Flags TCP;

3.2.93. Deve ter a capacidade de definir regras distintas para interfaces de rede distintas;

3.2.94. A solução deverá ser capaz de reconhecer e possibilitar o bloqueio de 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;

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

3.2.96. Para facilitar a criação e administração de regras de firewall, deve trabalhar com objetos que podem ser lista de ips, lista de MACs, lista de portas;

3.2.97. Regras de firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra

3.2.98. Regras de firewall poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

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

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

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

3.2.102. 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;

3.2.103. Deve ser possível trabalhar com prioridades diferentes, sendo que a prioridade maior prevalece sobre a prioridade menor;

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

3.2.105. Deverá permitir limitar o número de meias conexões vindas de um computador;

3.2.106. Deverá prevenir ack storm;

3.2.107. Deverão existir regras padrão da solução que possam ser utilizadas como modelo para a criação e adição de novas regras;

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

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

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

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

3.2.112. Deve 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;

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

3.2.114. Deve ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão;

3.2.115. Deve 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;

3.2.116. Deve ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;

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

3.2.118. Deve 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 fins de investigação do incidente;

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

3.2.120. Deve ser capaz de permitir ou negar que métodos utilizados por Webservers por regras de IPS;

3.2.121. Deve possibilitar que 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);

3.2.122. Deve possibilitar que regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

3.2.123. Deve ser capaz de inspecionar tráfego criptografado de entrada;

3.2.124. Deve 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;

3.2.125. Deve possibilitar que as regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;

3.2.126. Deve 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;

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

3.2.128. Deve 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;

3.2.129. Deve possibilitar que a solução seja 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;

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

3.2.131. 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;

3.2.132. As regras de IPS de vulnerabilidade deverão apresentar severidade baseada em CVEs;

3.2.133. As regras de IPS poderão ter sua capacidade de LOG desabilitado;

3.2.134. Deve possibilitar que as regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta;

3.2.135. As regras devem ser atualizadas automaticamente pelo fabricante;

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

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

3.2.138. Deve ser capaz de detectar mudanças de integridade em arquivos e diretórios do sistema operacional e aplicações terceiras;

3.2.139. Deve ser capaz de detectar mudanças no estado de portas em sistemas operacionais Linux;

3.2.140. Deve ter a capacidade de monitorar o status de serviços e processos do sistema operacional;

3.2.141. Deve ter a capacidade de monitorar mudanças efetuadas no registro do Windows;

3.2.142. Deve 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;

3.2.143. Deve 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;

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

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

3.2.146. Deve logar e colocar em relatório todas as modificações que ocorram;

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

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

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

3.2.150. Deve possibilitar que algumas regras possam ser modificadas pelo administrador para adequação ao seu ambiente.

3.2.151. A solução deverá permitir implantação de funcionalidade de inspeção de Logs nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX;

3.2.152. Deve 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;

3.2.153. Deve 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;

3.2.154. Deve permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;

3.2.155. Deve permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;

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

3.2.157. Deve possibilitar a criação de regras de inspeção de logs para aplicações customizadas;

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

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

3.2.160. Deverá logar cada violação e colocar em relatório todas as violações relevantes que ocorram;

3.2.161. As regras poderão ser modificadas por severidade de ocorrência de eventos;

3.2.162. As regras devem se atualizar automaticamente pelo fabricante;

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

3.2.164. Deverá possuir funcionalidade de controle de aplicações deverá ser realizado através de Hash, suportando no mínimo MD5, SHA1 e SHA256;

3.2.165. O agrupamento dos eventos deverá ser realizado pelo menos por Hash ou por máquina;

3.2.166. A solução deverá possuir um mecanismo ao qual permita a execução de aplicações e scripts automaticamente, sem intervenção manual, por um determinado período de tempo;

3.2.167. Deverá possuir integração com a plataforma de investigação e correlação de incidentes hospedada em nuvem do próprio fabricante, com data lake próprio para detecção e investigação de atividades maliciosas e suspeitas;

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

3.2.169. O fabricante da solução deve dispor de laboratório próprio para desenvolvimento de vacinas e motores e possuir analista dedicado a desenvolvimento de defesas contra ameaças e malwares. Esta informação deve ser comprovada pelo Fabricante através de documentação oficial;

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

3.2.171. A solução deverá permitir configuração de Single Sign-On (SSO) com suporte a SAML 2.0;

3.2.172. A solução deve prover diferentes níveis de administração e acesso a ferramenta para os usuários em pelo menos: Master Administrador, Administrator, Analista e Auditor;

3.2.173. Deve ser possível a customização de perfis de usuários baseados de forma granular

3.2.174. Deve permitir configuração de duplo fator de autenticação para acesso dos usuários à console de gerenciamento;

3.2.175. Deve registrar os logs de atividades realizados na console de gerência para fins de auditoria;

3.2.176. Ter capacidade de enviar os eventos e detecções para aplicações de SIEM e Syslog terceiros;

3.2.177. Deve armazenar eventos de detecção por pelo menos 30 dias, para fins de investigação;

3.2.178. Deve permitir configuração de notificações por e-mail (SMTP) para envio de alertas e notificações;

3.2.179. Possuir modelos pré-definidos pelo fabricante de atividades suspeitas e maliciosas para identificação e categorização de ameaças no ambiente;

3.2.180. A solução deve ser capaz de associar diferentes modelos de ameaças e associá-los a um único incidente de segurança;

3.2.181. Deve ter capacidade de apresentar informações relacionadas ao MITRE para cada um dos eventos detectados no ambiente, caso possuam;

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

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

3.2.184. Permitir tomar diferentes ações de resposta no ambiente, no mínimo: Isolar endpoints, bloquear contas de usuário e adicionar arquivos, URL's, domínios e IP's em listas de bloqueios.

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

3.2.186. Deve monitorar os status dos produtos integrados à plataforma de resposta à incidentes através da console de gerência.

3.2.187. A solução deve apresentar uma lista com todos os modelos de comportamentos pré-definidos que a solução possui;

3.2.188. Cada modelo deve possuir uma descrição e criticidade para auxiliar na identificação do risco e impacto de cada modelo;

3.2.189. Deve permitir ativar ou desativar qualquer modelo de detecção caso necessário;

3.2.190. Permitir criação de listas de exceção de objetos para redução de falso-positivo;

3.2.191. Os modelos de detecção deverão possuir níveis de severidade individuais para cada modelo em pelo menos os seguintes níveis:

3.2.191.1. Crítico;

3.2.191.2. Alto;

3.2.191.3. Médio;

3.2.191.4. Baixo.

3.2.192. Deve prover relatórios de inteligência de ameaças avançadas mais recentes e indicadores de comprometimento para ajudar sua organização a se defender proativamente contra ameaças;

3.2.193. Deve integrar relatórios de inteligência criados por especialistas em ameaças do fabricante e terceiros para ajudar na identificação de ameaças;

3.2.194. Os relatórios de ameaças do fabricante deverão gerar alertas de detecção caso sejam identificadas atividades presentes nos relatórios dentro do ambiente;

3.2.195. Deve ser possível identificar individualmente cada relatório de ameaça;

3.2.196. Deve permitir adicionar bases de inteligência terceiras de forma manual, por API, importando arquivos com base CSV ou STIX através de assinatura de feeds de inteligência de ameaças terceiros;

3.2.197. Deve permitir adicionar no mínimo os seguintes indicativos de comprometimento (IOCs) à base de inteligência:

3.2.197.1. SHA-1;

3.2.197.2. SHA-256

3.2.197.3. URLs;

3.2.197.4. IPs;

3.2.197.5. Domínios;

3.2.198. Deve permitir configurar as ações dos indicativos de comprometimento (IOCs) adicionados à console em pelo menos:

3.2.198.1. Log;

3.2.198.2. Bloquear/Enviar à quarentena;

3.2.199. A base de inteligência terceira deve ser integrada através dos protocolos TAXII 2.0 ou TAXII 2.1.

3.2.200. Deve fornecer mecanismos de gestão e governança que permitam a identificação e avaliação de riscos sobre os ativos da organização, em conformidade com as recomendações do NIST (National Institute of Standards and Technology).

3.2.200.1. A plataforma deve monitorar atributos de ativos e padrões de comportamento para avaliar o valor empresarial com base na tríade CIA conforme descrito no NIST SP 800-60.

3.2.200.2. Deve fornecer um índice global de risco.

3.2.200.3. Deve fornecer sugestões sobre as ações de remediação mais importantes para reduzir o risco geral.

3.2.200.4. Deve ser possível determinar quais alertas de risco serão desconsiderados na pontuação da organização e o período em que o risco será aceito.

3.2.200.5. Deve fornecer um índice de risco com base nas configurações de produtos integrados do fornecedor para reduzir o risco induzido por erros humanos.

3.2.200.6. A gestão da superfície de ataque deve ser integrada na plataforma, fornecendo informações sobre Dispositivos Internos, Ativos Voltados para a Internet, Contas e Aplicações na Nuvem.

3.2.200.7. Deve ser fornecido um painel para exibir todos os usuários/dispositivos com Alto Risco para tomada de ações.

3.2.200.8. Deve ser possível realizar benchmarking em tempo real com comparação de nível de risco.

3.2.200.9. Devem ser suportadas fontes de dados de terceiros para análises adicionais a nível de identidade, como Azure AD, Office 365, AD local.

3.2.200.10. Deve detectar o comprometimento de contas de usuário.

3.2.200.11. Deve detectar vulnerabilidades exploráveis do sistema operacional nos endpoints e servidores.

3.2.200.12. Deve fornecer um guia para reduzir fatores de risco detectados.

3.2.200.13. Deve permitir definir um objetivo de redução de risco.

3.2.200.14. Visualizar um resumo dos eventos de risco que você deve remediar para alcançar o objetivo selecionado e alterar o status dos eventos de risco.

3.2.200.15. Visualizar informações sobre os ativos que foram mais impactados por cada evento de risco.

3.2.200.16. Deve permitir as seguintes ações para responder a riscos: Desativar/Ativar conta do usuário - Forçar logout - Redefinir senha - Isolar/Restaurar Endpoint - Monitorar tentativas de login - Monitorar/Bloquear/Desbloquear/Permitir aplicativo interno - Bloquear/Desbloquear/Permitir Acesso a aplicativos ou URLs em nuvem.

3.2.200.17. Deve identificar as aplicações SaaS e locais de cada dispositivo.

3.2.200.18. Deve enumerar a superfície de ataque da CONTRATANTE, dependendo das fontes de dados conectadas, compreendendo:

3.2.200.19. As estações de trabalho, os servidores e os dispositivos móveis da CONTRATANTE

3.2.200.20. Os usuários da CONTRATANTE, apontando inclusive aqueles que detêm poderes administrativos

3.2.200.21. As aplicações acessadas por usuários e dispositivos da CONTRATANTE, apontando inclusive aquelas que passaram por recente vazamento de dados

3.2.200.22. Os ativos mantidos pela CONTRATANTE sob custódia de Provedores de Serviços em Nuvem

3.2.200.23. Os domínios da CONTRATANTE, suportando ao menos 10 domínios diferentes

3.2.200.24. Os subdomínios da CONTRATANTE

3.2.200.25. Os IPs Públicos associados à CONTRATANTE e seus respectivos hosts

3.2.200.26. As portas de comunicação/serviços abertos em cada host público

3.2.200.27. Deve prover dicas para mitigação dos riscos mapeados no ambiente da CONTRATANTE;

3.2.200.28. Deve indicar os principais eventos que devem ser mitigados para diminuir a pontuação de risco da CONTRATANTE;

3.2.200.29. A visibilidade de riscos deve detalhar quais são os principais alertas de segurança e associá-los às táticas do MITRE;

3.2.200.30. Deve ser possível identificar pontos de melhorias associados às camadas de proteção do ambiente da CONTRATANTE;

3.2.200.31. Deve ser possível listar melhorias a serem realizadas nas soluções de IAM da CONTRATANTE identificando, no mínimo, se há excesso de privilégios e se estão utilizando protocolo de autenticação vulnerável.

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

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

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

3.2.204. O campo de busca deve permitir o uso de múltiplos operadores lógicos para no mínimo:

3.2.204.1. E;

3.2.204.2. Ou;

3.2.204.3. Não;

3.2.205. Deve permitir indexar múltiplas buscas utilizando operadores lógicos;

3.2.206. Deve permitir salvar pesquisas com os critérios de busca e operadores lógicos utilizados para futuras consultas;

3.2.207. Deve permitir pesquisar por atividades de cada um dos contextos, mesmo que não tenham gerado qualquer tipo de detecção pelos modelos de detecção de ameaça;

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

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

3.2.210. Deve somar as pontuações de cada modelo durante a correlação das atividades para melhor categorização do incidente;

3.2.211. Deve exibir todos os detalhes do incidente em uma única página, contendo no mínimo:

3.2.211.1. Status do incidente;

3.2.211.2. Score;

3.2.211.3. Escopo impactado:

3.2.211.4. Quantidade de contas de e-mail impactadas;

3.2.211.5. Data e hora da detecção;

3.2.211.6. Técnica do MITRE utilizada;

3.2.211.7. Modelo(s) de detecção acionado(s);

3.2.211.8. Objetos detectados dentro de cada modelo;

3.2.212. Deve permitir alterar o status de cada evento, para no mínimo:

3.2.212.1. Novo;

3.2.212.2. Em progresso/análise;

3.2.212.3. Fechado;

3.2.212.4. Fechado – falso positivo;

3.2.213. Permitir adicionar comentários e notas a cada evento pelos analistas da ferramenta;

3.2.214. Durante o processo de análise da cadeia de processos deve ser possível verificar todos os objetos relacionados à esta análise, as atividades executadas pelos objetos e sua reputação conforme categorização do fabricante;

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

3.2.216. 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.

3.2.217. Permitir adicionar um comentário junto a cada ação tomada para registro e contextualização das ações;

3.2.218. Deve permitir adicionar arquivos SHA-1, SHA-256, URLs, IPs e domínios à lista de bloqueio dos sensores;

3.2.219. Deve permitir remover arquivos SHA-1, SHA-256, URLs, IPs ou domínios a lista de bloqueio dos sensores;

3.2.220. Permitir coletar e fazer o download de um arquivo para investigação local detalhada;

3.2.221. Permitir adicionar o remetente (sender) de um e-mail na lista de bloqueio, impedindo o mesmo de enviar novos e-mails os usuários da sua empresa;

3.2.222. Mover o e-mail selecionado para a área de quarentena de um específico usuário ou todos os usuários que contenham este e-mail em suas caixas;

3.2.223. Deletar o e-mail selecionado das caixas selecionadas;

3.2.224. Deve permitir verificar todas as ações de respostas executadas na console ou por API.

3.2.225. Deve ser possível automatizar ações de respostas

3.2.226. A solução deve prover templates para utilização de ação de resposta;

3.3. SOLUÇÃO DE SEGURANÇA TRENDMICRO PARA CONTAINERS E NUVEM COM MÓDULO DE DETECÇÃO E RESPOSTA A AMEAÇAS AVANÇADAS, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 24 (VINTE E QUATRO) MESES.

3.3.1. A solução deve ter capacidades de varredura de contêineres tanto em pré-execução quanto em tempo de execução.

3.3.2. A solução deve ser capaz de proteger contêineres durante todo o seu ciclo de vida (no momento da implantação, após a implantação, em tempo de execução).

3.3.3. A solução deve ajudar a resolver vulnerabilidades e outros problemas de segurança nas imagens de contêiner antes que possam ser explorados em produção.

3.3.4. A solução deve ser capaz de integrar a segurança ao pipeline de Integração Contínua e Entrega Contínua (CI/CD) sem interferir nos ciclos de desenvolvimento do CI/CD.

3.3.5. A solução deve suportar a varredura de templates de Infraestrutura como Código (IaC) com CloudFormation e Terraform.

3.3.6. A solução deve ser capaz de realizar varreduras em pré-execução em artefatos com suporte para os seguintes artefatos:

3.3.6.1. Imagens de contêiner

3.3.6.2. Arquivos binários

3.3.6.3. Diretórios com código-fonte

3.3.6.4. Arquivos OCI

3.3.7. A solução deve ser capaz de gerar uma Lista de Materiais de Software (SBOM) e retornar um relatório de vulnerabilidade após realizar uma varredura de vulnerabilidade nos resultados do SBOM.

3.3.8. A solução deve ser capaz de escanear imagens de contêiner como parte do seu pipeline de desenvolvimento e realizar varreduras contínuas de imagens em seus registros.

3.3.9. A solução deve suportar a funcionalidade de Controlador de Admissão baseado em políticas.

3.3.10. A solução deve ter uma opção para criar políticas personalizadas que permitam ou bloqueiem implantações com base em um conjunto de regras de controle de admissão definidas.

3.3.11. A solução deve ser capaz de integrar os resultados da varredura de artefatos nas políticas de controle de admissão de segurança de contêineres.

3.3.12. A solução deve suportar varredura de malware/ameaças em contêineres.

3.3.13. A solução deve ter capacidade de segurança em tempo de execução e deve ser capaz de fornecer alertas e indicadores de ataques (IoA) em aplicativos conteinerizados em execução.

3.3.14. A solução deve ter varredura de vulnerabilidade em tempo de execução de contêineres.

3.3.15. A solução deve suportar segurança em tempo de execução eBPF.

3.3.16. A solução deve ser capaz de coletar dados de atividade em tempo de execução de ativos em nuvem descobertos para fins de correlação e enriquecimento de XDR e sincronizar automaticamente os dados de volta para o console de gerenciamento em nuvem.

3.3.17. A solução deve fornecer visibilidade instantânea de VMs e contêineres em nuvem vulneráveis em execução.

3.3.18. A solução deve ter modelos de detecção predefinidos específicos para workloads e contêineres que combinam várias regras e filtros de eventos usando técnicas como aprendizado de máquina e empilhamento de dados. Deve ser regularmente atualizada para melhorar as capacidades de detecção de ameaças e reduzir alertas falsos positivos.

3.3.19. A solução deve ter a capacidade de habilitar ou desabilitar modelos de detecção e adicionar/configurar exceções de modelos de detecção dependendo das necessidades do seu ambiente.

3.3.20. A solução deve permitir a criação de modelos de detecção personalizados e filtros de eventos personalizados que definem os eventos que o modelo de detecção usa para acionar alertas.

3.3.21. A solução deve listar todos os Indicadores de Ataques (IOA) que estão mapeados no framework MITRE ATT&CK, o Analista SOC pode usar esses eventos como ponto de partida para realizar investigações adicionais.

3.3.22. O console deve fornecer diferentes métodos de busca, filtros e uma linguagem de consulta fácil de usar, semelhante ao Kibana, para identificar, categorizar e recuperar resultados de busca.

3.3.23. A solução deve ter a capacidade de buscar nos dados de atividade de Workload ou Contêiner e ser capaz de escrever consultas de busca personalizadas, adicionar as consultas salvas à lista de observação e executá-las automaticamente contra os dados de telemetria mais recentes em intervalos regulares.

3.3.24. A solução deve ser capaz de gerar um alerta de workbench e apresentar uma análise de causa raiz – incluindo TTPs associados do MITRE ATT&CK – e identificar o escopo do impacto em ativos em nuvem.

3.3.25. A solução deve ter um chatbot com IA (Companheiro de IA) para orientar nas investigações e fornecer automaticamente respostas a quaisquer perguntas relacionadas à cibersegurança. A solução deve permitir que ações de resposta sejam tomadas a partir do menu de contexto diretamente da investigação do Workbench.

3.3.26. A solução deve ser capaz de tomar ações de resposta para conter incidentes dentro da sua conta em nuvem, como revogar o acesso de usuários IAM suspeitos.

3.3.27. A solução deve suportar ações de resposta adicionais aproveitando a integração com sistemas de ticketing de terceiros.

3.3.28. A solução deve suportar Playbooks de Segurança para mudar de respostas manuais para fluxos de trabalho automatizados, ajudar a reduzir a carga de trabalho e acelerar tarefas e investigações de segurança.

3.3.29. A solução precisa incluir a capacidade de construir playbooks de segurança contra ameaças e riscos, como bloquear a atividade de um arquivo, desligar um endpoint, desconectar um endpoint da internet, colocar arquivos em quarentena, excluir arquivos maliciosos, etc.

3.3.30. A solução deve ter a capacidade de criar playbooks do zero ou usar templates integrados, dependendo das necessidades do seu ambiente.

3.3.31. A solução deve suportar monitoramento XDR da sua conta em nuvem (AWS CloudTrail) para obter insights acionáveis sobre a atividade de usuários, serviços e recursos com modelos de detecção identificando atividades como escalonamento de privilégios, modificação de senhas e outras técnicas de ataque.

3.3.32. A solução deve ser capaz de se integrar com uma plataforma de cibersegurança que seja capaz de gerenciar a Segurança de Endpoint, Email, Nuvem, Rede, OT, XDR e Zero Trust da organização em um único console.

3.3.33. A solução deve fornecer um painel altamente personalizável que fornece widgets exibindo estatísticas de Superfície de Ataque, Email, Endpoint, Rede, SecOps, XDR e Nuvem.

3.4. SOLUÇÃO DE VISIBILIDADE DE REDE COM FUNCIONALIDADE DE DETECÇÃO E RESPOSTA A AMEAÇAS AVANÇADAS, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 24 MESES

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

3.4.1.1. Deve ser dimensionada para inspecionar 10 Gbps de throughput;

3.4.1.2. Deve possuir pelo menos uma interface de gerenciamento dedicada 10/100/1000 base-T;

3.4.2. Deve possuir pelo menos quatro interfaces de 10Gb SFP+ para análise de tráfego;

3.4.3. Deve possuir fonte redundante;

3.4.4. Deve possuir no máximo 2RU (Rack Unit);

3.4.5. Não serão aceitos appliances de Unified Threat Management (UTM) e Next-Generation Firewall (NGFW) para monitoramento do tráfego, ainda que possua recurso e licenciamento específico para análise de ameaças em rede;

3.4.6. Funcionalidades e Requisitos específicos:

3.4.6.1. 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:

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

3.4.6.3. Detecção de ataques direcionados;

3.4.6.4. Analisador de ameaças em nuvem;

3.4.6.5. Correlação de regras para detecção de conteúdo malicioso;

3.4.6.6. Análise de todos os estágios de uma sequência de ataques.

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

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

3.4.7.2. 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;

3.4.7.3. Permitir a detecção da conta de um usuário vazado na dark web.

3.4.7.4. Permitir o fornecimento de informações sobre contas de usuários que apresentarem atividades anômalas de alto risco ou que foram especificamente alvo de campanhas de e-mail maliciosas.

3.4.7.5. Permitir a detecção de vulnerabilidades exploráveis do sistema operacional.

3.4.7.6. 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;

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

3.4.7.8. 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 worms 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;

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

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

3.4.8. Permitir a rápida identificação da criticidade dos eventos de segurança;

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

3.4.10. 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;

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

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

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

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

3.4.15. A capacidade de análise de artefatos em sandbox pode ser realizada através de integração com serviço em nuvem do próprio fabricante;

3.4.16. A solução deverá possuir mecanismo de conhecimento de senhas de pelo menos 90 palavras chaves em seu vocabulário de conhecimento, para derivação de arquivos protegidos;

3.4.17. Capacidade de criar e salvar investigações customizadas dos incidentes de segurança;

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

3.4.19. 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;

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

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

3.4.22. 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, 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; Messenger, GPass, IP, ARP, TCP, UDP e IGMP;

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

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

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

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

3.4.27. 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;

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

3.4.29. 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;

3.4.30. 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;

3.4.31. A análise de sandbox deve identificar e analisar ameaças que tenham características de evitar a segurança e análise em ambiente simulado, auto-preservação e roubo de dados.

3.4.32. 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;

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

3.4.34. 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);

3.4.35. Deverá analisar arquivos maliciosos na rede utilizando vacinas e técnicas de heurística;

3.4.36. Deve possuir foco em proteção contra APTs (Advanced Persistent Threats);

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

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

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

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

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

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

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

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

3.4.45. Deve atuar de forma passiva na captura de tráfego sem oferecer impacto no desempenho da rede;

3.4.46. Deve possuir interface web para busca e investigação local de incidentes;

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

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

3.4.49. A solução deve possuir recurso de prevenção de ameaças avançadas, com capacidade de apresentar em seus logs, visibilidade de acordo com o framework ATT&CK MITRE Matrix, pontuando características de táticas e técnicas de acordo com a ameaça detectada/bloqueada pela solução;

3.4.50. 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;

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

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

3.4.52.1. Resumidos;

3.4.52.2. Visão Geral dos Incidentes de Segurança

3.4.52.3. Discriminação dos Tipos de Incidentes

3.4.52.4. Top Ameaças Analisadas

3.4.52.5. Top Hosts Infectados

3.4.52.6. Recomendações de Segurança

3.4.52.7. Executivos;

3.4.52.8. Deve possuir detalhes técnicos dos incidentes detectados;

3.4.52.9. Deve possuir estatística do tráfego analisado;

3.4.52.10. Deve possuir indicadores de risco do ambiente;

3.4.52.11. Recomendações de Segurança.

3.4.53. 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;

3.4.54. 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.;

3.4.55. 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;

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

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

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

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

3.4.60. Deve ser capaz de detectar propagação de malwares na rede;

3.4.61. Deve ser capaz de detectar tentativas de brute-force;

3.4.62. Deve ser capaz de detectar tentativas de fuga e roubo de informação;

3.4.63. Deve ser capaz de detectar ameaças que se replicam na rede;

3.4.64. Deve ser capaz de detectar Exploits na rede;

3.4.65. O Monitoramento de protocolos de comunicação deve ser feito através de appliance único;

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

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

3.4.68. Deve permitir consultas personalizáveis, usando comandos SQL ou atributos pré-definidos;

3.4.69. Capacidade de salvar uma investigação antes de ser finalizada;

3.4.70. Capacidade de restaurar uma investigação para continuá-la ou consultá-la;

3.4.71. Capacidade de emitir relatórios baseados nas investigações;

3.4.72. Deve permitir apresentação dos dados consultados em vários formatos, incluindo tabela e gráficos;

3.4.73. Deve trabalhar com geo-localização para identificar a origem geográfica de um ataque;

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

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

3.4.76. Deve sugerir consultas a bases de reputação e whois quando encontrados hosts e nomes de domínio;

3.4.77. Deve permitir recebimento de logs via syslog;

3.4.78. Deve permitir encaminhamento de logs via syslog;

3.4.79. Deve permitir receber logs de diferentes dispositivos;

3.4.80. Deve possuir engine de correlação de eventos;

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

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

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

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

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

3.4.86. 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;

3.4.87. 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;

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

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

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

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

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

3.4.93. 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:

3.4.93.1. Uso de CPU

3.4.93.2. Uso de Disco;

3.4.93.3. Uso de Memória;

3.4.93.4. Tráfego malicioso analisado;

3.4.93.5. Todo o tráfego analisado.

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

3.4.94.1. Tipo de evento de detecções: Conteúdo malicioso, reputação de URL's, comportamentos maliciosos, comportamentos suspeitos, Exploits, correlações de eventos, Grayware;

3.4.94.2. Tipo de eventos de sistemas: Eventos de sistema e eventos de atualizações.

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

3.4.96. 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;

3.4.97. 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 trânsito através de logs de sensor;

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

3.4.98.1. Computadores infectados;

3.4.98.2. Origem de infecções;

3.4.98.3. Estatísticas de ameaças;

3.4.98.4. Riscos potenciais de segurança;

3.4.98.5. Riscos de perda de informações;

3.4.98.6. Risco de sistema comprometido;

3.4.98.7. Risco de disseminação de ameaças;

3.4.98.8. Eventos suspeitos;

3.4.98.9. Infecções de malware.

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

3.4.99.1. Critérios de pesquisa por dia, mês e ano.

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

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

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

3.4.100. A solução deverá possuir funcionalidade de Detecção e Resposta do mesmo fabricante com as seguintes características:

3.4.100.1. Deve ter a capacidade de integrar-se com a plataforma de detecção e resposta centralizada existente, a fim de enviar objetos suspeitos e metadados das detecções locais para correlação com as demais soluções de segurança do ambiente;

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

3.4.100.3. Deve permitir a integração dos eventos ocorridos em outros segmentos de rede e outros appliances com objetivo de correlacionar os ataques na rede;

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

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

3.4.100.6. 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 de estações de trabalho ou servidores, sem acréscimos ou mudanças de licenciamento;

3.4.100.7. Deve ser compatível com os sistemas operacionais Windows, Linux e MacOS;

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

3.4.100.9. Deve possuir módulo de investigação e detecção integrados;

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

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

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

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

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

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

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

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

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

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

3.4.100.20. Deve permitir que as detecções sejam correlacionadas com módulos de servidores e estações de trabalho através de console centralizada existente.

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

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

3.4.100.23. Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;

3.4.100.24. 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;

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

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

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

3.4.100.28. 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;

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

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

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

3.4.100.32. 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;

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

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

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

3.4.100.36. 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;

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

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

3.4.100.39. 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;

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

3.4.100.41. Deve permitir adicionar arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores;

3.4.100.42. Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores;

3.4.100.43. Deve permitir terminar processos ativos executados nas estações de trabalhos e servidores;

3.4.100.44. Permitir coletar e fazer o download de um arquivo para investigação local detalhada;

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

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

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

3.4.100.48. 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.

3.5. DOS SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO DE VISIBILIDADE DE REDE.

3.5.1. A CONTRATADA deverá instalar e configurar a solução a ser fornecida com as seguintes atividades:

3.5.1.1. Planejamento da implementação, considerando:

- Topologia de rede do Datacenter do IPLAN, e demais órgãos interconectados na rede coporativa de serviços;
- Segmentos de rede (VLANs) que serão monitorados;
- Banda de rede necessária para a inspeção do tráfego de rede, no cenário de implementação “Out-of-Band”, compatível com o appliance de hardware fornecido;

3.5.1.2. Instalação física do Equipamento no Rack e conexão das interfaces de rede com o switch Core no Datacenter a CONTRATANTE.

3.5.1.3. Ativação do produto e integração com a console de administração centralizada em nuvem (SaaS) existente;

3.5.1.4. Criação de políticas e regras de detecção dentro das melhores práticas de segurança de acordo com o fabricante;

3.5.1.5. Definição das políticas e regras de detecção levando em consideração as necessidades e restrições de cada órgão ou entidade da Prefeitura do Rio de Janeiro;

3.5.1.6. Entrega da documentação das configurações das soluções de visibilidade de rede implementada (As Built);

3.5.1.7. Suporte especializado para administração das soluções de visibilidade de rede e ajustes pós-implementação;

3.5.2. Para prestação destes serviços, a CONTRATADA deverá empregar funcionário(s) devidamente qualificado(s) na instalação, configuração, administração e utilização da solução.

3.5.3. O serviço em questão deve atuar em conjunto com o suporte especializado do fabricante na implementação, manutenção e aplicação das melhores práticas no ambiente.

3.6. DO SERVIÇO DO TÉCNICO RESIDENTE

3.6.1.1. Os serviços de técnico residente serão prestados de segunda-feira a sexta-feira nas instalações da CONTRATANTE, no horário compreendido entre 09:00hs e 18:00hs, nos dias úteis e pontos facultativos, exceto sábados, domingos e feriados.

3.6.1.2. O técnico residente deverá possuir formação de nível superior em Tecnologia da Informação ou afins, sólidos conhecimentos em segurança da informação e na solução ofertada.

3.6.1.2.1. A comprovação deve ser feita mediante a apresentação em até 05 dias úteis após a celebração do contrato da cópia dos seguintes documentos:

3.6.1.2.2. Diploma de conclusão de nível superior (Tecnólogo ou Bacharel) em Tecnologia da Informação.

3.6.1.2.3. Certificação CompTIA Security+: Competency in system security, network infrastructure, access control and organizational security.

3.6.1.2.4. Cópia de Certificado emitido pelo Fabricante que comprove sólidos conhecimentos na solução de Visibilidade de Rede e Detecção e Resposta ofertada.

3.6.1.3. Serão desconsideradas certificações eventualmente vencidas, ou sem a atualização devida;

3.6.1.4. São competências do técnico residente:

3.6.1.4.1. Colaborar ativamente no desenvolvimento e implementação de estratégias de visibilidade de ameaças de rede.

3.6.1.4.2. Promover a melhoria contínua dos níveis de eficiência, eficácia e efetividade na utilização da solução CONTRATADA;

3.6.1.4.3. Auxiliar o corpo técnico no uso pleno dos recursos oferecidos pela solução contratada..

4 DA FUNDAMENTAÇÃO LEGAL DA CONTRATAÇÃO

A presente contratação tem fundamento na Lei Federal n.º 13.303/2016, no Decreto Municipal n.º 44.698/2018, no Regulamento de Licitações e Contratos

da IPLANRIO – RLC IPLANRIO, disponível no Portal da Prefeitura do Rio de Janeiro: https://iplanrio.prefeitura.rio/contratos-e-licitacoes/, bem como nas regras procedimentais acerca da modalidade de pregão eletrônico, dispostas na Lei Federal n.º14.133/2021.

5 DA QUALIFICAÇÃO TÉCNICA

5.1. Prova de aptidão da empresa licitante para desempenho de atividade pertinente e compatível com o objeto da licitação, por meio de certidão (ões) ou atestado(s), fornecido(s) por pessoa jurídica de direito público ou privado.

5.2. Será admitida a soma dos atestados ou certidões apresentadas pelas licitantes, desde que os mesmos sejam tecnicamente pertinentes e compatíveis em características, quantidades e prazos com o objeto da licitação.

5.3. Considera-se compatível com o objeto da licitação a apresentação de atestado de capacidade técnica que comprove a prestação de serviço para no mínimo 50% do quantitativo previsto neste Termo de Referência;

6 DAS OBRIGAÇÕES DA CONTRATANTE

São obrigações da CONTRATANTE:

6.1. Realizar os pagamentos na forma e condições previstas;

6.2. Realizar a fiscalização do objeto deste Termo de Referência.

7 DAS OBRIGAÇÕES DA CONTRATADA

São obrigações da CONTRATADA:

7.1. Realizar os serviços de acordo com todas as exigências contidas no Termo de Referência e na proposta;

7.2. Tomar as medidas preventivas necessárias para evitar danos a terceiros, em consequência da execução dos serviços;

7.3. Responsabilizar-se integralmente pelo ressarcimento de quaisquer danos e prejuízos, de qualquer natureza, que causar à CONTRATANTE ou a terceiros, decorrentes da execução do objeto desta contratação, respondendo por si, seus empregados, prepostos e sucessores, independentemente das medidas preventivas adotadas e da comprovação de sua culpa ou dolo na execução do contrato;

7.4. Atender as determinações e exigências formuladas pela CONTRATANTE;

7.5. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, efeitos ou incorreções resultantes da execução ou de materiais empregados, no prazo determinado pela Fiscalização;

7.6. Responsabilizar-se, na forma do Contrato, por todos os ônus, encargos e obrigações comerciais, sociais, tributárias, trabalhistas e previdenciárias, ou quaisquer outras previstas na legislação em vigor, bem como por todos os gastos e encargos com material e mão de obra necessária à completa execução dos serviços:

a) em caso de ajuizamento de ações trabalhistas contra a CONTRATADA, decorrentes da execução do presente Contrato, com a inclusão do Município do Rio de Janeiro ou da CONTRATANTE como responsável

subsidiário ou solidário, a CONTRATANTE poderá reter, das parcelas vincendas, o montante dos valores cobrados, que serão complementados a qualquer tempo com nova retenção em caso de insuficiência;

b) no caso da existência de débitos tributários ou previdenciários, decorrentes da execução do presente Contrato, que possam ensejar responsabilidade subsidiária ou solidária da CONTRATANTE, as parcelas vincendas poderão ser retidas até o montante dos valores cobrados, que serão complementados a qualquer tempo com nova retenção em caso de insuficiência;

c) as retenções previstas nas alíneas “a” e “b” poderão ser realizadas tão logo tenha ciência o Município do Rio de Janeiro ou a CONTRATANTE da existência de ação trabalhista ou de débitos tributários e previdenciários e serão destinadas ao pagamento das respectivas obrigações caso o Município do Rio de Janeiro ou entidade da Administração Pública indireta sejam compelidos a tanto, administrativa ou judicialmente, não cabendo, em nenhuma hipótese, ressarcimento à CONTRATADA;

d) eventuais retenções previstas nas alíneas “a” e “b” somente serão liberadas pela CONTRATANTE se houver justa causa devidamente fundamentada.

7.7. Manter as condições de habilitação e qualificação exigidas para a contratação durante todo prazo de execução contratual;

7.8. Responsabilizar-se, na forma do Contrato, pela qualidade dos serviços executados e dos materiais empregados, em conformidade com as especificações do Termo de Referência, com as normas da Associação Brasileira de Normas Técnicas – ABNT, e demais normas técnicas pertinentes, a ser atestada pelos responsáveis pela fiscalização da execução do contrato, assim como pelo refazimento do serviço e a substituição dos materiais recusados, sem ônus para o(a) CONTRATANTE e sem prejuízo da aplicação das sanções cabíveis;

7.9. Responsabilizar-se inteira e exclusivamente pelo uso regular de marcas, patentes, registros, processos e licenças relativas à execução desta contratação, eximindo a CONTRATANTE das consequências de qualquer utilização indevida;

7.10. Indicar, nas notas fiscais emitidas, quando o objeto envolver prestação de serviços, o efetivo período do mês que está sendo faturado.

8 DA ENTREGA DAS LICENÇAS / SUBSCRIÇÕES

A disponibilização das Licenças / subscrições e das credenciais de acesso para o console web do módulo de Administração das soluções de Proteção de Servidores, Container, Nuvem e de Visibilidade de Rede com funcionalidade de detecção e resposta a ameaças avançadas do fabricante, especificadas nos itens 1, 2 e 3, deverão ser encaminhadas por mensagem eletrônica à CONTRATANTE (dop.gsc@prefeitura.rio)

9 DOS PRAZOS

9.1. O prazo de validade da Ata de Registro de Preços será de 12 (doze) meses.

9.2. O prazo de vigência da contratação será de 24 (vinte e quatro) meses, contados a partir da assinatura do contrato, podendo ser prorrogado, nos termos da legislação em vigor.

9.3. O prazo de garantia técnica dos serviços será de 24 (vinte e quatro) meses, contados a partir da disponibilização das Licenças / subscrições e das credenciais de acesso para o console web do módulo de Administração das Soluções constantes nos itens 1, 2 e 3.

9.4. O prazo de disponibilização das Licenças / subscrições e das credenciais de acesso para o console web do módulo de Administração das Soluções constantes nos itens 1, 2 e 3 será de 10 (dez) dias úteis contados a partir da assinatura do contrato.

9.5. O prazo para início dos serviços de instalação e configuração da solução ofertada será de 05 (cinco) dias úteis após disponibilização das Licenças / subscrições e das credenciais de acesso para o console web do módulo de Administração da Solução de Segurança para proteção de e-mail.

10 DA GARANTIA CONTRATUAL

10.1. A CONTRATADA prestará garantia de 2% (dois por cento) do valor total do Contrato, como determina o art. 457 do RGCAF, a ser prestada antes do ato de assinatura, em uma das modalidades previstas no art. 445 do RGCAF e no art. 91 do Regulamento de Licitações e Contratos da IplanRio – RLC IPLANRIO. Seus reforços poderão ser igualmente prestados nas mesmas modalidades. Caso o fornecedor escolha a modalidade seguro-garantia, esta deverá incluir a cobertura das multas eventualmente aplicadas, e, caso escolha a modalidade carta-fiança, deverá observar as regras descritas na Portaria IPLANRIO "N" Nº 153, de 09 de fevereiro de 2011.

10.2. A CONTRATANTE se utilizará a garantia para assegurar as obrigações associadas à contratação, podendo recorrer a esta inclusive para cobrar valores de multas eventualmente aplicadas e ressarcir-se dos prejuízos que lhe forem causados em virtude do descumprimento das referidas obrigações. Para reparar esses prejuízos, poderá a CONTRATANTE ainda reter créditos.

10.3. Os valores das multas impostas por descumprimento das obrigações assumidas na contratação serão descontados da garantia caso não venham a ser quitados no prazo de 03 (três) dias úteis, contados da ciência da aplicação da penalidade. Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, responderá a CONTRATADA pela diferença, que será descontada dos pagamentos eventualmente devidos pela Administração ou cobrada judicialmente.

10.4. Em caso de rescisão decorrente de falta imputável à CONTRATADA, a garantia reverterá integralmente à CONTRATANTE, que promoverá a cobrança de eventual diferença que venha a ser apurada entre o importe da garantia prestada e o débito verificado.

10.5. Na hipótese de descontos da garantia a qualquer título, seu valor original deverá ser integralmente recomposto no prazo de 7 (sete) dias úteis, exceto no caso da cobrança de valores de multas aplicadas, em que esse será de 48 (quarenta e oito) horas, sempre contados da utilização ou da notificação pela CONTRATANTE, o que ocorrer por último, sob pena de rescisão administrativa do Contrato.

10.6. Caso o valor da contratação seja alterado, de acordo com o art. 92 do Decreto Municipal 44.698/2028, a CONTRATADA deverá complementar o valor da garantia para que seja mantido o percentual de 2% (dois por cento) do valor do Contrato.

10.7. Sempre que houver reajuste ou alteração do valor da contratação, a garantia será complementada no prazo de 7 (sete) dias úteis do recebimento, pela CONTRATADA, do correspondente aviso, sob pena de aplicação das sanções previstas no RGCAF.

10.8. A garantia contratual só será liberada ou restituída com o integral cumprimento da contratação, mediante ato liberatório da autoridade contratante, de acordo com o art. 465 do RGCAF e, quando em dinheiro, atualizada monetariamente.

11 DA FISCALIZAÇÃO E ACEITE DO OBJETO

11.1. A CONTRATADA submeter-se-á a todas as medidas e procedimentos de Fiscalização. Os atos de fiscalização, inclusive inspeções e testes, executados pela CONTRATANTE e/ou por seus prepostos, não eximem a CONTRATADA de suas obrigações no que se refere ao cumprimento das normas, especificações e projetos, nem de qualquer de suas responsabilidades legais e contratuais.

11.2. A Fiscalização da execução do (s) serviço (s) caberá à comissão designada por ato da autoridade competente no âmbito da Empresa Municipal de Informática S/A - IPLANRIO. Incumbe à Fiscalização a prática de todos os atos que lhe são próprios nos termos da legislação em vigor, respeitados o contraditório e a ampla defesa.

11.3. A CONTRATADA declara, antecipadamente, aceitar todas as decisões, métodos e processos de inspeção, verificação e controle adotados pela CONTRATANTE, se obrigando a fornecer os dados, elementos, explicações, esclarecimentos e comunicações de que este necessitar e que forem considerados necessários ao desempenho de suas atividades.

11.4. A CONTRATADA se obriga a permitir que o pessoal da fiscalização da CONTRATANTE acesse quaisquer de suas dependências, possibilitando o exame das instalações e também das anotações relativas aos equipamentos, pessoas e materiais, fornecendo, quando solicitados, todos os dados e elementos referentes à execução do contrato.

11.5. Compete à CONTRATADA fazer minucioso exame das especificações do (s) serviço (s), de modo a permitir, a tempo e por escrito, apresentar à Fiscalização, para o devido esclarecimento, todas as divergências ou dúvidas porventura encontradas e que venham a impedir o bom desempenho do Contrato. O silêncio implica total aceitação das condições estabelecidas.

11.6. A atuação fiscalizadora em nada restringirá a responsabilidade única, integral e exclusiva da CONTRATADA no que concerne ao (s) serviço (s) contratado (s), à sua execução e às consequências e implicações, próximas ou remotas, perante a CONTRATANTE, ou perante terceiros, do mesmo modo que a ocorrência de eventuais irregularidades na execução contratual não implicará corresponsabilidade da CONTRATANTE ou de seus prepostos.

11.7. A aceitação do objeto deste Termo de Referência se dará mediante a avaliação de Comissão de Fiscalização designada pela autoridade competente no âmbito da Empresa Municipal de Informática S/A – IPLANRIO, e constituída na forma do art. 501, do RGCAF, que constatará se os serviços executados atendem a todas as especificações contidas neste Termo ou no processo que ensejou a presente contratação.

11.8. O objeto do presente Termo de Referência será recebido em tantas parcelas quantas forem as relativas ao pagamento.

11.9. Os serviços cujos padrões de qualidade estejam em desacordo com a especificação contida neste Termo e seus anexos deverão ser recusados pela Comissão responsável pela fiscalização do contrato, que anotará em registro próprio as ocorrências e determinará o que for necessário à regularização das faltas ou defeitos observados. No que exceder à sua competência, comunicará o fato à autoridade superior, em 5 (cinco) dias, para ratificação.

11.10. Na hipótese de recusa de aceitação, por não atenderem às exigências da CONTRATANTE, a CONTRATADA deverá reexecutar quaisquer serviços defeituosos ou qualitativamente inferiores, passando a contar os prazos para pagamento e demais compromissos da CONTRATANTE da data da efetiva aceitação. Caso a CONTRATADA não reexecute os serviços não aceitos no prazo assinado, a CONTRATANTE se reserva o direito de providenciar a sua execução às expensas da CONTRATADA, sem prejuízo das penalidades cabíveis.

11.11. O Aceite Provisório ficará a cargo da Comissão de Fiscalização, que emitirá Termo de Aceitação Provisória em até 10 (dez) dias, após a entrega das licenças/subscrições descritos neste Termo de Referência.

12 DO SUPORTE TÉCNICO

12.1. Os serviços deverão ter garantia pelo prazo indicado no subitem 9.2.

12.2. O Suporte Técnico deverá ser prestado para cada solução fornecida e deverá ser acionada em caso de qualquer indisponibilidade da solução, conforme os índices de criticidade abaixo:

Criticidade	Descrição	Prazo Máximo de Atendimento	Objetivo de Restauração de Serviço
Severidade 1 (Alta)	Solução parada ou inoperante comprometendo sua eficácia do serviço de visibilidade de rede contra ameaças	Em até 30 min. Deve ser iniciado o atendimento através de transferência ao telefone.	Restauração do serviço referente à solução contratada em até 6 dias corridos.
Severidade 2 (Média/Alta)	Comprometimento parcial da solução, gerando restrição de funcionalidades. A solução continua funcionando, porém, de forma limitada.	Em até 2 horas deve ser iniciado o atendimento através de transferência ao telefone ou retorno de chamada.	Restauração do serviço referente à solução contratada em até 10 dias corridos.
Severidade 3 (Média/Baixa)	O defeito não gera impacto às funcionalidades da solução. Exemplo: ocorreu um erro que causou um impacto negativo limitado.	Em até 6 horas deve ser iniciado o atendimento através de transferência ao telefone ou retorno de chamada	Restauração do serviço referente à solução contratada em até 15 dias corridos ou na próxima atualização do Software
Severidade 4 (Baixa)	O problema é pequeno, ou de acesso à documentação. Exemplos: o problema não afetou as operações da contratante de forma relevante; Encaminhamento de solicitações de orientação técnica ou sugestões para novos recursos ou aprimoramentos da solução.	No mesmo dia ou no próximo dia útil comercial.	Restauração do serviço referente à solução contratada em até 20 dias corridos ou considerado para as próximas atualizações da solução.

12.3. O atendimento deve estar disponível para todos os produtos que compõem a solução;

12.4. O suporte Técnico relativo ao hardware e às subscrições adquiridas deverá contemplar a atualização de versão (upgrades de software) para novas versões e patches e suporte técnico, publicados durante o período de vigência do contrato, sem ônus para a CONTRATANTE.

12.5. Para eventos caracterizados como Severidade 1 ou Severidade 2, conforme descritos na tabela acima, deverão ser disponibilizadas até 4 visitas presenciais solicitadas sob demanda, para cada período de 12 (doze) meses, em regime 24 x 7 x 120 para resolução dos chamados, atividades proativas com acesso as ferramentas de propriedade exclusivas do fabricante para análise de capacidade e reparos;

12.6. Para a abertura de chamados, a CONTRATADA deverá disponibilizar canais de acesso 24 (vinte e quatro) horas por dia e 7(sete) dias por semana, através de número de telefone de discagem gratuita e internet para abertura de chamados técnicos objetivando a resolução de problemas e dúvidas quanto ao funcionamento da solução.

12.7. Todos os chamados, independente de sua criticidade, deverão ser abertos em um único número telefônico.

12.8. Todos os prazos para atendimento da garantia começarão a ser contados a partir da abertura do chamado independentemente de este ter sido feito via telefone, e-mail ou Web.

12.9. Dentro do prazo máximo de solução está compreendido o prazo de atendimento;

12.10. Considera-se plenamente solucionado o problema quando restabelecidos os sistemas/serviços sem restrições, ou seja, quando não se tratar de uma solução paliativa;

12.11. Os serviços de atendimento para chamados de severidades 1 e 2 não podem ser interrompidos até o completo restabelecimento de todas as funções comprometidas, mesmo que para isso o atendimento tenha que se estender por períodos noturnos e dias não úteis (sábados, domingos e feriados);

12.12. Nos casos em que as manutenções necessitarem de paradas da solução, o CONTRATANTE deverá ser imediatamente notificado para que se proceda à aprovação da manutenção, ou para que seja agendada nova data, a ser definida pelo CONTRATANTE, para execução das atividades de manutenção;

12.13. A CONTRATADA deve emitir relatórios de todas as intervenções realizadas, preventivas e corretivas, programadas ou de emergência, ressaltando os fatos importantes e detalhando os pormenores das intervenções, de forma a manter registros completos das ocorrências e subsidiar as decisões da administração do Complexo Central de Tecnologia do CONTRATANTE;

12.14. O relatório deve ser assinado por representante do CONTRATANTE, responsável pelo acompanhamento do serviço, que se obriga a acompanhar a execução das manutenções;

12.15. Não haverá custos adicionais para a CONTRATANTE, quando da abertura dos chamados técnicos.

12.16. Em caso de descumprimento dos prazos descrito na tabela do item 12.2, a Contratada se sujeitará às penalidades previstas no Edital e no Contrato.

13 DAS CONDIÇÕES DE PAGAMENTO

13.1. O pagamento das soluções especificadas nos itens 1, 2 e 3.1 , serão efetuado à CONTRATADA em 01 (uma única) parcela à vista após a regular liquidação da despesa, nos termos do art. 63 da Lei Federal nº 4.320/64, observada a regras de recebimento do objeto contidas no RLC IPLANRIO e neste Termo de Referência. O prazo para pagamento será de 30 (trinta) dias, contados da data do protocolo do documento de cobrança no setor competente do(a) CONTRATANTE e obedecido o disposto na legislação.

13.2. O pagamento dos Serviços de Instalação e configuração da solução de visibilidade de rede especificados no item 3.2 será efetuado à CONTRATADA em 01 (uma única) parcela à vista, após ateste dos serviços e regular liquidação da despesa, nos termos do art. 63 da Lei Federal nº 4.320/64, observada a regras de recebimento do objeto contidas no RLC IPLANRIO e neste Termo de Referência. O prazo para pagamento será de 30 (trinta) dias, contados da data do protocolo do documento de cobrança no setor competente do(a) CONTRATANTE e obedecido o disposto na legislação.

a) O ateste dos serviços pela área técnica competente será emitida em até 05 (cinco) dias úteis após a entrega dos serviços.

13.3. O pagamento dos serviços de Técnico Residente descritos no item 3.3 será efetuado à CONTRATADA mensalmente, após ateste dos serviços e regular liquidação da despesa, nos termos do art. 63 da Lei Federal nº 4.320/64, observada a regras de recebimento do objeto contidas no RLC IPLANRIO e neste Termo de Referência. O prazo para pagamento será de 30 (trinta) dias, contados da data do protocolo do documento de cobrança no setor competente do(a) CONTRATANTE e obedecido o disposto na legislação.

13.4. Para fins de medição, se for o caso, e faturamento, o período-base de medição do serviço prestado será de um mês, considerando- se o mês civil, podendo no primeiro mês e no último, para fins de acerto de contas, o período se constituir em fração do mês, considerado para esse fim o mês com 30 (trinta) dias.

13.5. O pagamento à CONTRATADA será realizado em razão dos serviços efetivamente prestados e aceitos no período-base mencionado no item anterior sem que o(a) CONTRATANTE esteja obrigado(a) a pagar o valor total do Contrato.

13.6. A CONTRATADA deverá apresentar juntamente com o documento de cobrança, os comprovantes de recolhimento do FGTS e INSS de todos os empregados atuantes no contrato, assim como Certidão Negativa de Débitos Trabalhistas – CNDT ou Certidão Positiva de Débitos Trabalhistas com efeito negativo válida, declaração de regularidade trabalhista, na forma do Anexo do Edital.

13.7. O valor dos pagamentos eventualmente efetuados com atraso, desde que não decorra de fato ou ato imputável à CONTRATADA, sofrerá a incidência de juros calculados de acordo com a variação da Taxa Selic, pro rata die entre o 31º (trigésimo primeiro) dia da data do protocolo do documento de cobrança no setor competente da CONTRATANTE e a data do efetivo pagamento, limitado ao percentual de 12% (doze por cento) ao ano.

13.8. O valor dos pagamentos eventualmente antecipados será descontado à taxa de 1% (um por cento) ao mês, calculada pro rata die, entre o dia do pagamento e o 30º (trigésimo) dia da data do protocolo do documento de cobrança no setor competente do (a) CONTRATANTE.

13.9. O pagamento será efetuado à CONTRATADA através de crédito em conta bancária do fornecedor cadastrado junto à Coordenação do Tesouro Municipal.

14 DAS SANÇÕES ADMINISTRATIVAS

14.1. Sem prejuízo de indenização por perdas e danos, a IplanRio poderá impor ao contratado, pelo descumprimento total ou parcial das obrigações a que esteja sujeito, as seguintes sanções, observado o Regulamento Geral do Código de Administração Financeira e Contabilidade Pública do Município do Rio de Janeiro – RGCAF e o Regulamento de Licitações e Contratos da IplanRio, garantida a defesa prévia ao contratado:

I advertência;
II Multa de mora de até 1% (um por cento) por dia útil sobre o valor do Contrato ou do saldo não atendido do Contrato;
III Multa de até 20% (vinte por cento) sobre o valor do Contrato ou do saldo não atendido do Contrato, conforme o caso, e, respectivamente, nas hipóteses de descumprimento total ou parcial da obrigação, inclusive nos casos de rescisão por culpa da CONTRATADA;
IV suspensão temporária do direito de licitar e impedimento de contratar com a Administração Municipal;

14.2. A multa aplicada será depositada em conta bancária indicada pela IplanRio, descontada dos pagamentos eventualmente devidos, descontada da garantia ou cobrada judicialmente.

14.3. As sanções previstas nos incisos I e IV do subitem 14.1 poderão ser aplicadas juntamente com as dos incisos II e III, devendo a defesa prévia do interessado, no respectivo processo, ser apresentada no prazo de 10 (dez) dias úteis e não excluem a possibilidade de rescisão unilateral do contrato;

14.4. Do ato que aplicar a pena prevista no inciso IV do subitem 14.1, a autoridade competente no âmbito da CONTRATANTE dará conhecimento aos demais órgãos e entidades municipais interessados, na página oficial desta empresa pública na internet.

14.5. A sanção prevista no inciso IV do subitem 14.1 poderá também ser aplicada às empresas ou aos profissionais que, em razão dos contratos regidos pelo Decreto Municipal n.º 44.698/2018:

I - tenham sofrido condenação definitiva por praticarem, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;
II - tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

III - demonstrem não possuir idoneidade para contratar com a IplanRio em virtude de atos ilícitos praticados.

14.6. As multas previstas nos incisos II e III do subitem 14.1 não possuem caráter compensatório, e, assim, o pagamento delas não eximirá a CONTRATADA de responsabilidade pelas perdas e danos decorrentes das infrações cometidas.

14.7. As multas aplicadas poderão ser compensadas com valores devidos à CONTRATADA mediante requerimento expresso nesse sentido.

14.8. Ressalvada a hipótese de existir requerimento de compensação devidamente formalizado, nenhum pagamento será efetuado à CONTRATADA antes da comprovação do recolhimento da multa ou da prova de sua relevação por ato da Administração, bem como antes da recomposição do valor original da garantia, que tenha sido descontado em virtude de multa imposta, salvo decisão fundamentada da autoridade competente que autorize o prosseguimento do processo de pagamento.

15 DA MATRIZ DE RISCOS

15.1. Para a presente contratação foram identificados os principais riscos conhecidos na Matriz constante do Anexo II deste Termo de Referência, bem como estabelecidos os respectivos responsáveis e descritas suas respostas sugeridas.

15.2. É vedada a celebração de aditivos decorrentes de eventos supervenientes alocados na Matriz de Riscos como sendo de responsabilidade da CONTRATADA.

15.3. Sempre que atendidas as condições do contrato e mantidas as disposições da Matriz de Risco, considera-se mantido o equilíbrio econômico-financeiro.

15.4. A proposta comercial deverá ser elaborada levando em consideração a natureza e a extensão dos riscos relacionados na Matriz de Risco.

16 DA PROPOSTA DE PREÇOS

16.1. A pretensa CONTRATADA deverá apresentar proposta de preços de acordo com as especificações deste Termo de Referência e nos moldes praticados pelo Município do Rio de Janeiro.

16.2. Os preços propostos deverão estar de acordo com os praticados no mercado e neles deverão estar inclusos todos os impostos, taxas, fretes, material, mão de obra, instalações e quaisquer outras despesas necessárias e não especificadas neste Termo de Referência, mas julgadas essenciais ao cumprimento do objeto desta contratação, observando-se, ainda, o contido no subitem 15.4 deste Termo de Referência.

17 DO TIPO DE LICITAÇÃO

17.1. O tipo de licitação será o menor preço global.

17.2. Os itens do escopo de fornecimento possuem correlação entre si e são elementos inseparáveis de uma mesma e única solução de TI para prover o gerenciamento, monitoramento, verificação e proteção dos emails. A separação por item dá-se apenas para clareza na composição dos preços, portanto não se deve ter duas empresas distintas prestando os serviços de integração dos sistemas, que fazem parte da contratação.

17.3. O regime de empreitada será por preço Global

Rio de Janeiro, 15 de novembro de 2025.

Leonardo Cavalieri

Matrícula: 40/622.627-9

Gerente de Segurança Cibernética

IPLANRIO/DOP

_____

Jorge Francisco Antunes da Silva

Matrícula: 40/2622163-4

Diretor de Operações

IPLANRIO

Anexo I - MATRIZ DE RISCO

ANEXO II - MATRIZ DE RISCOS

Identificação dos Riscos					Análise Qualitativa			Resposta aos Riscos (Tratamento)		
Id.	**Tipo**	**Risco**	**Categoria**	**Sub Categoria**	**P**	**I**	**P x I**	**Estratégia**	**Resposta Sugerida**	**Responsável**
R001	Ameaça	Devido a variação cambial, pode haver aumento dos custos dos produtos importados	Organizacional	Aquisição	8	8	**64**	Mitigar	A contratada deverá considerar a variação cambial em sua proposta de preço	Contratada
R002	Ameaça	Devido ao calendário orçamentário da PCRJ, pode haver atraso no pagamento do contrato	Organizacional	Aquisição	7	9	**6 3**	Mitigar	A contratada deverá manter fluxo de caixa para cobrir o período descoberto	Contratada
R004	Ameaça	Devido a alteração da política econômico-financeira, pode haver aumento nos tributos após a contratação	Organizacional	Aquisição	4	5	**20**	Aceitar Ativamente	A contratada deverá buscar alternativas para cumprimento do contrato	Contratada
R005	Ameaça	Monitoramento do ambiente, devido à ausência de mão de obra qualificada	Organizacional	Aquisição	9	9	**81**	Mitigar	Ampliar quadro técnico e capacitar para grupo de trabalho com foco exclusivo na monitoração	Contratante
R006	Ameaça	Devido ao atraso de pagamento do contrato, a equipe da contratada poderá levar ao atraso no atendimento do serviço	Organizacional	Aquisição	7	8	**56**	Mitigar	Deverá manter fluxo de caixa para cobrir o período descoberto	Contratada
R007	Ameaça	Reduzir a indisponibilidade do ambiente de TI, reagir de forma eficiente na detecção de ameaças de segurança no ambiente de TI	Técnico	Segurança	9	9	**81**	Mitigar	Implementar a solução de DDI para monitoração do ambiente em ferramenta confiável	Contratante