CÂMARA MUNICIPAL DE
SÃO CAETANO DO SUL

TERMO DE REFERÊNCIA

OBJETO: O presente PREGÃO tem por objeto a contratação de empresa especializada em serviços segurança e comunicação da informação para fornecimento de solução para Rede de Dados Core, Wi-Fi, Segurança Cibernética, incluindo operação de NOC (Network Operations Center) e SOC (Security Operations Center) 24x7x365, com monitoramento contínuo, análise e desenvolvimento de correções de vulnerabilidades, bem como suporte e garantia de equipamentos de TIC (Tecnologia da Informação e Comunicação), para os trabalhos de forma continua e segura desenvolvidos nesta edilidade, conforme caracterizado nas especificações técnicas de cada item presente neste Termo de Referência.

Deverão ser apresentados juntamente com a proposta comercial **CATÁLOGOS, ENCARTES, FOLHETOS TÉCNICOS, COMPROVAÇÃO DE HOMOLOGAÇÃO PELA ANATEL ATRAVÉS DA NUMERAÇÃO DE CONSULTA E MANUAIS** dos equipamentos, softwares e serviços ofertados, onde constem as especificações técnicas e a descrição detalhadados equipamentos, softwares, componentes, acessórios e demais itens que compõe a solução, permitindo a consistente avaliação dos itens.

O prazo de ativação será de até **60 (sessenta) dias,** após a emissão da ordem de serviços.

O serviço deverá ser prestado durante o período de **24 (vinte e quatro) meses** podendo ser prorrogado por iguais períodos nos termos da lei.

LOTE ÚNICO	
ITEM	**DESCRIÇÃO**
1	SERVIÇO ESPECIALIZADO DE SWITCHES CORE
2	PLATAFORMA DE GESTÃO E CONECTIVIDADE PARA WI-FI
3	SERVIÇO DE SEGURANÇA CIBERNÉTICA
4	SUPORTE TÉCNICO E MONITORAMENTO
5	SERVIÇO DE INSTALAÇÃO

DESCRIÇÃO DOS SERVIÇOS

1. SERVIÇO ESPECIALIZADO DE SWITCHES CORE

1.1. O serviço compreende o fornecimento, implantação, configuração e ativação de switches de núcleo (Core Switches) destinados à infraestrutura de rede do Data Center, com o objetivo de garantir alta disponibilidade, desempenho, escalabilidade e segurança no tráfego de dados da rede corporativa.

1.2. A solução deverá contemplar a instalação física dos equipamentos em rack padrão de Data Center, bem como a implementação de uma arquitetura de rede baseada em redundância e alta

disponibilidade, assegurando a continuidade dos serviços mesmo em casos de falhas de hardware ou enlaces.

1.3. Os switches core deverão ser configurados para operar como camada central da rede, realizando a agregação dos switches de distribuição e acesso, além de suportar roteamento de camada 3 (Layer 3), segmentação de rede por VLANs, protocolos de redundância e balanceamento de tráfego.

1.4. O serviço de fornecimento e implantação de switches deverá atender integralmente aos requisitos técnicos estabelecidos neste documento.

1.5. Deverá ser entregue uma solução em alta disponibilidade (redundância), contemplando todos os equipamentos e acessórios necessários para o pleno funcionamento da infraestrutura, incluindo, mas não se limitando a patch cords, módulos GBIC/SFP, cabos DAC e demais componentes, de forma a garantir a completa integração e configuração no cenário atual do ambiente.

1.6. Switch deverá ser gerenciável Layer 3 em formato 1U.

1.7. Deve possuir 48 portas RJ45 auto-sensing com suporte a 10/100/1000 Mbps.

1.8. Deve possuir 4 portas SFP+ integradas de 10GbE para conectividade de alta velocidade.

1.9. Deve possuir 2 portas uplink QSFP28 com suporte a 100GbE para agregação de alta capacidade.

1.10. Deve possuir arquitetura non-blocking, suportando switching em velocidade de linha para camadas 2 e 3.

1.11. Deve possuir capacidade de switching de 280 Gbps (half duplex).

1.12. Deve suportar taxa de encaminhamento de até 800 milhões de pacotes por segundo (Mpps).

1.13. Deve suportar taxa de dados de até 570 Gbps full duplex.

1.14. Deve possuir 16 GB de memória DDR4.

1.15. Deve possuir no mínimo 32 GB de armazenamento SSD interno.

1.16. Deve possuir buffer de pacotes mínimo de 8 MB.

1.17. Deve suportar até 4.000 VLANs por sistema.

1.18. Deve suportar até 4.000 membros de VLAN por sistema.

1.19. Deve suportar no mínimo 8.000 endereços MAC.

1.20. Deve possuir porta de gerenciamento out-of-band 10/100/1000BASE-T.

1.21. Deve possuir porta USB tipo A para configuração através de dispositivo flash.

1.22. Deve possuir porta de console Micro-USB (Type B) e porta de console RJ45 com sinalização RS-232.

1.23. Deve suportar auto-negociação de velocidade e controle de fluxo, além de Auto-MDI/MDIX.

1.24. Deve suportar port mirroring e espelhamento baseado em fluxo.

1.25. Deve suportar controle de tempestade de broadcast (Broadcast Storm Control).

1.26. Deve suportar Energy Efficient Ethernet (EEE) com configuração por porta.

1.27. Deve utilizar modelo de switching Store-and-Forward.

1.28. Deve suportar fontes de alimentação internas redundantes e hot-swappable.

1.29. Deve utilizar fonte de alimentação de 550W certificada 80PLUS Platinum.

1.30. Deve possuir ventoinhas redundantes com velocidade variável.

1.31. Deve suportar fluxo de ar normal ou reverso.

1.32. Deve possuir duas imagens de firmware armazenadas internamente.

1.33. Deve suportar VRF Lite permitindo múltiplos roteadores virtuais no mesmo switch físico.

1.34. Deve suportar IPv4 e IPv6 incluindo BGP, OSPFv2/v3, VRF, BFD, PIM-SSM e IGMP.

1.35. Deve suportar VXLAN para virtualização de rede.

1.36. Deve suportar MLAG para alta disponibilidade e utilização total de banda.

1.37. Deve suportar atualização de firmware sem necessidade de desligar a rede.

1.38. Deve suportar AAA, TACACS+ e autenticação RADIUS.

1.39. Deve suportar interface OpenConfig gNMI para gerenciamento do sistema.

1.40. Deve suportar Private VLAN e Private VLAN Edge.

1.41. Deve incluir kit de montagem para rack de 2 postes.

1.42. Deve possuir consumo máximo de energia de até 212 W.

1.43. Deve possuir saída térmica máxima de 340,00 BTU/h.

1.44. Deve possuir eficiência mínima de 88% em todos os modos de operação.

1.45. Deve operar em temperaturas entre 0°C e 45°C.

1.46. Deve suportar temperaturas de armazenamento entre -40°C e 65°C.

1.47. Deve operar com umidade relativa em até 90% sem condensação.

1.48. Deve suportar umidade em até 95% sem condensação.

1.49. Deve incluir cabos de alimentação C13 para NEMA 5-15 com comprimento de 3 metros e C13 para C14 com comprimento de 2 metros.

1.50. O equipamento com bandejas de ventilação e uma fonte AC instalada deve possuir peso aproximado de 7 kg (15.43 lb).

1.51. O equipamento com bandejas de ventilação e duas fontes de alimentação instaladas deve possuir peso aproximado de 8,3 kg.

1.52. Deve suportar controle de acesso à rede baseado em IEEE 802.1X, além de autenticação através de RADIUS e TACACS+.

1.53. Deve suportar gerenciamento via Command Line Interface (CLI) para configuração e monitoramento do equipamento.

1.54. Deve suportar SNMP (Simple Network Management Protocol) para integração com sistemas de monitoramento de rede.

1.55. Deve suportar gerenciamento e automação através de APIs REST.

1.56. Deve suportar arquitetura de rede aberta (Open Networking) permitindo flexibilidade na escolha do sistema operacional de rede.

1.57. A fonte de alimentação deve possuir eficiência mínima de 80% em todos os modos de operação.

1.58. Deve possuir saída térmica máxima de aproximadamente 1000.00 BTU/h.

1.59. Deve suportar temperatura de armazenamento entre -40°C e 70°C.

1.60. A solução proposta, deverá conter todos os cabos, gbic, e itens necessários para o bom funcionamento do ambiente computacional da Câmara Municipal de São Caetano do Sul.

2. PLATAFORMA DE GESTÃO E CONECTIVIDADE PARA WI-FI

2.1. A solução consiste em uma plataforma de gerenciamento de acesso à rede sem fio baseada em portal cativo (Captive Portal), destinada ao controle, autenticação, monitoramento e gestão de usuários que utilizam redes Wi-Fi em ambientes corporativos ou públicos.

2.2. O sistema deve permitir que dispositivos conectados à rede sejam automaticamente redirecionados para uma página de autenticação web, antes de obter acesso à internet ou aos recursos da rede, garantindo controle sobre os usuários e conformidade com políticas de segurança e uso aceitável.

2.3. A plataforma deverá possuir interface de administração centralizada, permitindo o gerenciamento de políticas de acesso, autenticação de usuários, criação de páginas personalizadas de login e acompanhamento em tempo real das conexões e atividades da rede.

2.4. A solução deve ser fornecida no modelo SaaS, sem a necessidade de adicionais de hardware, permitindo escalabilidade, atualizações contínuas, e implementação e suporte técnico remoto.

2.5. A plataforma deve estar em conformidade com o Marco Civil da Internet.

2.6. A plataforma deve estar em conformidade com a Lei Geral de Proteção de Dados (LGPD), incluindo coleta e armazenamento seguro de dados de visitantes.

2.7. A plataforma deve ser agnóstica ao hardware, com capacidade de integração nativa com as principais marcas de mercado.

2.8. Deve permitir a importação e exportação de dados via APIs, facilitando a comunicação com sistemas internos e externos.

2.9. A plataforma deve gerenciar os processos de credenciamento, autenticação e contabilidade de dispositivos e usuários.

2.10. A plataforma deve processar e integrar dados de estacionamento, clima e faturamento, além de calcular ticket médio automaticamente.

2.11. Deve oferecer um painel de controle configurável e dinâmico, permitindo personalizações por parte do administrador.

2.12. Deve permitir a segmentação de público por comportamento e perfil, facilitando ações de marketing e análise de clientes.

2.13. A plataforma deve ser capaz de identificar visitas cruzadas entre diversos locais frequentados pelos mesmos usuários.

2.14. Deve permitir cruzar dados de diversas fontes no painel de controle para gerar relatórios avançados.

2.15. A plataforma deverá possibilitar a extração de relatórios e criação de envios automatizados.

2.16. Gerar relatórios de total de acesso ao wifi, total de registros, tempo médio de acesso ao wifi, usuários novos e retornantes, download e upload de dados (tráfego de dados)

2.17. A plataforma deve permitir o envio de e-mails, SMS, vídeos e PUSH automaticamente ou via API, além de se integrar com sistemas externos de envio de e-mails e SMS e WhatsApp.

2.18. A plataforma deve contar com um Captive Portal personalizável, sem a necessidade de senha para acesso inicial, capaz de:

2.19. Coletar informações solicitadas aos usuários durante o cadastro.

2.20. Apresentar múltiplas perguntas para enriquecimento de perfil dos usuários.

2.21. Reproduzir vídeos e personalizar o conteúdo com base no perfil do usuário.

2.22. Realizar pesquisas de opinião e ser editável via HTML, CSS e Javascript.

2.23. Identificar automaticamente o idioma do dispositivo do usuário e exibir o conteúdo em seu idioma e sendo nativo o PT-BR.

2.24. A plataforma deve conseguir identificar e processar dados de presença dos visitantes, analisando:

2.25. Tempo de permanência e frequência de visitas.

2.26. Diferenciação entre visitantes e funcionários.

2.27. Contact tracing: identificação de usuários que visitaram diversos pontos.

2.28. Processamento de dados para mapa de calor e análise de fluxo.

2.29. Gestão de ocupação, com alertas automáticos e visualização em tempo real.

3. SERVIÇO DE CIBERSEGURANÇA PARA INFRAESTRUTURA DE REDES.

3.1. A solução deverá atender todos os requisitos deste termo de referência.

3.2. Todos os componentes que fazem parte da solução, de segurança para servidores, estações de trabalho deverão ser fornecidas por um único fabricante. Não serão aceitas composições de produtos de fabricantes diferentes;

3.3. A console de monitoração e configuração deverá ser feita através de uma central única, baseada em web e em nuvem, que deverá conter todas a fermentas para a monitoração e controle da proteção dos dispositivos;

3.4. A console de nuvem deve possuir o armazenamento de seus dados dentro do território nacional, garantindo conformidade e compliance com as leis locais como a LGPD, Instrução normativa 5 e NC-14 determinada pelo Banco Central;

3.5. A console deverá apresentar Dashboard com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional;

3.6. Deve possuir mecanismo de comunicação via API, para integração com outras soluções de segurança, como por exemplo SIEM;

3.7. Deve possuir capacidade de realizar a integração com soluções de firewalls para criar políticas automáticas em caso de ataques em massa nos computadores e servidores;

3.8. A console deve permitir a divisão dos computadores, dentro da estrutura de gerenciamento em grupos;

3.9. Deve permitir sincronização com o Active Directory (AD) para gestão de usuários e grupos integrados às políticas de proteção.

3.10. Deve possuir a possibilidade de aplicar regras diferenciadas baseado em grupos ou usuários;

3.11. A instalação deve ser feita via cliente específico por download da gerência central ou também via email de configuração. O instalador deverá permitir a distribuição do cliente via Active Directory (AD) para múltiplas máquinas;

3.12. Deve a console ser capaz de criar e editar diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários, não importando em que equipamentos eles estejam acessando;

3.13. Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos;

3.14. Deve permitir exclusões de escaneamento para um determinado websites, pastas, arquivos ou aplicações, tanto a nível geral quanto específico em uma determinada política.

3.15. A console de gerenciamento deve permitir a definição de grupos de usuários com diferentes níveis de acesso as configurações, políticas e logs;

3.16. Atualização incremental, remota e em tempo-real, da vacina dos Antivírus e do mecanismo de verificação (Engine) dos clientes;

3.17. Permitir o agendamento da varredura contra vírus com a possibilidade de selecionar uma máquina, grupo de máquinas ou domínio, com periodicidade definida pelo administrador;

3.18. Atualização automática das assinaturas de ameaças (malwares) e políticas de prevenção desenvolvidas pelo fabricante em tempo real ou com periodicidade definida pelo administrador;

3.19. Utilizar protocolos seguros padrão HTTPS para comunicação entre console de gerenciamento e clientes gerenciados.

3.20. As mensagens geradas pelo agente deverão estar no idioma em português ou permitir a sua edição.

3.21. Permitir a exportação dos relatórios gerenciais para os formatos CSV e PDF;

3.22. Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento;

3.23. Possibilidade de exibir informações como nome da máquina, versão do antivírus, sistema operacional, versão da engine, data da vacina, data da última verificação, eventos recentes e status;

3.24. Capacidade de geração de relatórios, estatísticos ou gráficos, tais como:

3.25. Detalhar quais usuários estão ativos, inativos ou desprotegidos, bem como detalhes dos mesmos;

3.26. Detalhamento dos computadores que estão ativos, inativos ou desprotegidos, bem como detalhes das varreduras e dos alertas nos computadores;

3.27. Detalhamento dos periféricos permitidos ou bloqueados, bem como detalhes de onde e quando cada periférico foi usado;

3.28. Detalhamento das principais aplicações bloqueadas e os servidores/usuários que tentaram acessá-las;

3.29. Detalhamento das aplicações permitidas que foram acessadas com maior frequência e os servidores/usuários que as acessam;

3.30. Detalhamento dos servidores/usuários que tentaram acessar aplicações bloqueadas com maior frequência e as aplicações que eles tentaram acessar;

3.31. Detalhamento de todas as atividades disparadas por regras de prevenção de perda de dados.

3.32. Deverá possuir um elemento de comunicação para mensagens e notificações entre estações e a console de gerenciamento utilizando comunicação criptografada;

3.33. Deve fornecer solução de gerenciamento de arquivos armazenados em nuvem, garantindo que um arquivo que foi feito um upload (exemplo Dropbox), tenha o processo monitorado e gerenciado, bem como realizar automaticamente o escaneamento do arquivo contra malwares, procuradas palavras chaves ou informações confidenciais. Deve ser bloqueado o upload ou removida a informação confidencial antes do envio do arquivo;

3.34. As portas de comunicação deverão ser configuráveis. A comunicação deverá permitir QoS para controlar a largura de banda de rede.

3.35. A solução deverá permitir a seleção da versão do software de preferência, permitindo assim o teste da atualização sobre um grupo de PCs piloto antes de implantá-lo para toda a rede. Permitir ainda selecionar um grupo de computadores para aplicar a atualização para controlar a largura de banda de rede. A atualização da versão deverá ser transparente para os usuários finais.

3.36. O agente anti-vírus deverá proteger laptops, desktops e servidores em tempo real, sob demanda ou agendado para detectar, bloquear e limpar todos os vírus, trojans, worms e spyware. No Windows o agente também deverá detectar PUA, adware, comportamento suspeito, controle de aplicações e dados sensíveis. O agente ainda deve fornecer controle de dispositivos terceiros e, controle de acesso a web;

3.37. Deve possuir mecanismo contra a desinstalação do endpoint pelo usuário e cada dispositivo deverá ter uma senha única, não sendo autorizadas soluções com senha única válida para todos os dispositivos;

3.38. Deve prover no endpoint a solução de HIPS (Host Instrusion Prevention System) para a detecção automática e proteção contra comportamentos maliciosos (análise de comportamento) e deverá ser atualizado diariamente;

3.39. Deve prover proteção automática contra web sites infectados e maliciosos, assim como prevenir o ataque de vulnerabilidades de browser via web exploits;

3.40. Deve permitir a monitoração e o controle de dispositivos removíveis nos equipamentos dos usuários, como dispositivos USB, periféricos da própria estação de trabalho e redes sem fio, estando sempre atrelado ao usuário o controle e não ao dispositivo;

3.41. O controle de dispositivos deve ser ao nível de permissão, somente leitura ou bloqueio;

3.42. Os seguintes dispositivos deverão ser, no mínimo, gerenciados: HD (hard disks) externos, pendrives USB, storages removíveis seguras, CD, DVD, Blu-ray, floppy drives, interfaces de rede sem fio, modems, bluetooth, infra-vermelho, MTP (Media Transfer Protocol) tais como Blackberry, iPhone e Android smartphone e PTP (Picture Transfer Protocol) como câmeras digitais;

3.43. A ferramenta de administração centralizada deverá gerenciar todos os componentes da proteção para estações de trabalho e servidores e deverá ser projetada para a fácil administração, supervisão e elaboração de relatórios dos endpoint e servidores;

3.44. Deverá possuir interface gráfica web, com suporte a língua portuguesa (padrão brasileiro);

3.45. A Console de administração deve incluir um painel com um resumo visual em tempo real para verificação do status de segurança;

3.46. Deverá fornecer filtros pré-construídos que permitam visualizar e corrigir apenas os computadores que precisam de atenção;

3.47. Deverá exibir os PCs gerenciados de acordo com critérios da categoria (detalhes do estado do computador, detalhes sobre a atualização, detalhes de avisos e erros, detalhes do antivírus, etc), e classificar os PCs em conformidade;

3.48. Uma vez que um problema seja identificado, deverá permitir corrigir os problemas remotamente, com no mínimo as opções abaixo:

- Proteger o dispositivo com a opção de início de uma varredura;
- Forçar uma atualização naquele momento;
- Ver os detalhes dos eventos ocorridos;
- Executar verificação completa do sistema;
- Forçar o cumprimento de uma nova política de segurança;
- Mover o computador para outro grupo;
- Apagar o computador da lista;

3.49. Atualizar a políticas de segurança quando um computador for movido de um grupo para outro manualmente ou automaticamente;

3.50. Gravar um log de auditoria seguro, que monitore a atividade na console de gerenciamento para o cumprimento de regulamentações, auditorias de segurança, análise e solução de problemas forenses;

3.51. Deverá permitir exportar o relatório de logs de auditoria nos formatos CSV e PDF;

3.52. Deve conter vários relatórios para análise e controle dos usuários e endpoints. Os relatórios deverão ser divididos, no mínimo, em relatórios de: eventos, usuários, controle de aplicativos, periféricos e web, indicando todas as funções solicitadas para os endpoints;

3.53. Fornecer relatórios utilizando listas ou gráficos, utilizando informações presentes na console, com no mínimo os seguintes tipos:

- Nome do dispositivo;
- Início da proteção;

- Último usuário logado no dispositivo;
- Último update;
- Último escaneamento realizado;
- Status de proteção do dispositivo;
- Grupo a qual o dispositivo faz parte;

3.54. Permitir a execução manual de todos estes relatórios danos formatos CSV e PDF;

3.55. A console deve possuir métodos de verificação da saúde das configurações da console, possibilitando aos administradores descobrirem facilmente se existe alguma falha de configuração que pode facilitar a entrada de malwares e invasores no ambiente;

CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE PROTEÇÃO PARA ESTAÇÕES DE TRABALHO

3.56. Características básicas do agente de proteção contra malwares:

3.57. Pré-execução do agente para verificar o comportamento malicioso e detectar malware desconhecido;

3.58. O agente deve buscar algum sinal de malware ativo e detectar malwares desconhecidos;

3.59. O agente deve ter a capacidade de submeter o arquivo desconhecido à nuvem de inteligência do fabricante para detectar a presença de ameaças;

3.60. O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;

3.61. A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;

3.62. Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de boot;

3.63. Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados;

3.64. Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);

3.65. Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;

3.66. Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;

3.67. É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs);

3.68. Suportar máquinas com arquitetura 32-bits e 64-bits (Exceto para Windows 11 que não há opção de 32bits;

3.69. O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais, macOS 12 Monterey, macOS 13 Ventura, macOS 14 Sonoma, macOS 15 Sequoia, Microsoft Windows 7, 8.1, 10 e 11;

3.70. Para macOS a solução deve ser compatível com a execução nativa em processadores Apple Silicon, não serão aceitas soluções que dependem de emulação via Rosetta2 da Apple.

3.71. Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;

3.72. Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção;

3.73. Funcionalidade de Firewall e Detecção e Proteção de Intrusão (IDS\IPS) com as funcionalidades:

3.74. Deverá possui atualização periódica de novas assinaturas de ataque;

3.75. Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo ou dinamicamente através do nome da aplicação.

3.76. Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;

3.77. Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.

3.78. Ser capaz de aplicar uma análise adicional, inspecionando finamente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como buffer overflow.

3.79. Deve possuir técnicas de proteção, que inclui:

3.80. Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;

3.81. Algorítimo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificados como um vírus;

3.82. Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;

3.83. Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);

3.84. Verificação de ameaças web avançadas: bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados;

3.85. Funcionalidade de Antivírus e AntiSpyware:

3.86. Proteção em tempo real contra vírus, trojans, worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos.

3.87. Proteção anti-malware deverá ser nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

3.88. As configurações do anti-spyware deverão ser realizadas através da mesma console do antivírus;

3.89. Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto;

3.90. Permitir a varredura das ameaças da maneira manual, agendada e em tempo real na máquina do usuário;

3.91. Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus;

3.92. Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção;

3.93. A remoção automática dos danos causados deverá ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante;

3.94. Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;

3.95. Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;

3.96. Antivírus de Web (verificação de sites e downloads contra vírus);

3.97. Controle de acesso a sites por categoria;

3.98. Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Safari, Opera e Chrome), fornecendo controle da Internet independentemente do browser utilizado, como parte da solução de proteção a estações de trabalho, incluindo a análise do conteúdo baixado pelo navegador web, de forma independente do navegador usado, ou seja, sem utilizar um plugin, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites.

3.99. O Controle da Web deve controlar o acesso a sites impróprios, com no mínimo 14 categorias de sites inadequados. Deve ainda permitir a criação de lista branca de sites sempre permitidos e lista negra de sites que devem ser bloqueados sempre;

3.100. Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio;

3.101. Capacidade de verificar somente arquivos novos e alterados;

3.102. Funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

3.103. Funcionalidade de detecção Pró-Ativa de reconhecimento de novas ameaças:

3.104. Funcionalidade de detecção de ameaças via técnicas de machine learning;

3.105. Deve prover de funcionalidade avançada de proteção preditiva baseada em inteligência artificial e machine learning, capaz de ajustar automaticamente políticas de segurança com base em comportamentos suspeitos e ameaças emergentes, para que possa reduzir a superfície de

ataque ao ativar controles adaptativos de acordo com o contexto do ambiente, sem a necessidade de intervenção manual constante.

3.106. A solução de proteção contra ameaças e demais recursos da solução devem funcionar em Modo de segurança do Windows;

3.107. Funcionalidade de detecção de ameaças desconhecidas que estão em memória;

3.108. Capacidade de detecção, e bloqueio pró-ativo de keyloggers e outros malwares não conhecidos (ataques de dia zero) através da análise de comportamento de processos em memória (heurística);

3.109. Capacidade de detecção e bloqueio de Trojans e Worms, entre outros malwares, por comportamento dos processos em memória;

3.110. Capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada.

3.111. Funcionalidade de proteção contra ransomwares:

3.112. Para estações de trabalho, dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;

3.113. Para estações de trabalho, dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares;

3.114. A Solução deve ter a capacidade de reverter automaticamente arquivos afetados por ransomware durante a sua execução em tempo real, através de uma tecnologia proprietária sem depender de VSS (Volume Shadow Copy);

3.115. Para servidores, dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação;

3.116. A solução deverá previnir ameaças e interromper que eles sejam executadas em dispositivos da rede, detectando e limpando os malwares, além da realização de uma análise detalhada das alterações realizadas.

3.117. Deve possuir uma tecnologia anti-exploit baseada em comportamento, reconhecendo e bloqueando as mais comuns técnicas de malware, protegendo os endpoints de ameaças desconhecidas e vulnerabilidades zero-day.

3.118. Deve ser realizada a detecção e o bloqueio de, pelo menos, as seguintes técnicas de exploit:

- DEP (Data Execution Prevention);
- Address Space Layout Randomization (ASLR);
- Bottom Up ASLR;
- Null Page;
- Anti-HeapSpraying;
- Dynamic Heap Spray;
- Import Address Table Filtering (IAF);
- VTable Hijacking;

- Stack Pivot and Stack Exec;
- SEHOP;
- Stack-based ROP (Return-Oriented Programming);
- Control-Flow Integrity (CFI);
- Syscall;
- WOW64;
- Load Library;
- Shellcode;
- VBScript God Mode;
- Application Lockdown;
- Process Protection;
- Network Lockdown.

3.119. A solução deverá trabalhar silenciosamente na máquina do usuário e deverá detectar a criptografia maliciosa de dados (ransomware), realizando a sua interrupção. No caso de arquivos serem criptografados a solução deverá realizar o retorno destes arquivos ao seu estado normal. Deste modo a solução deve ser capaz de fazer a limpeza e remoção completa do ransomware na máquina do usuário.

3.120. Deve fornecer também uma análise detalhada das modificações realizadas pelo ransomware, realizando a correlação dos dados em tempo real, indicando todas as modificações feitas em registros, chaves, arquivos alvos, conexões de redes e demais componentes contaminados.

3.121. A console de monitoração e configuração deverão ser feitas através de uma central única, baseada em web e em nuvem, que deverá conter todas a ferramentas para a monitoração e controle da proteção dos dispositivos para a solução de anti-exploit e anti-ransomware.

3.122. A console deverá apresentar Dashboard com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional, bem como todas as identificações para o mapeamento instantâneo dos efeitos causados pelo ransomware nos endpoints.

SOLUÇÃO DE ENDPOINT DETECTION AND RESPONSE (EDR)

3.123. A solução deve ter capacidade de implementar técnicas de EDR (Endpoint Detection and Response), possibilitando detecção e investigação nos endpoints com atividades suspeitas;

3.124. Deve ter a capacidade de submeter arquivos identificados em incidentes a uma segunda consulta a nuvem de inteligência do fabricante.

3.125. Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do malware e o ponto final de bloqueio.

3.126. Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:

3.127. Detalhes do Processo, como nome, hash, hora e data da detecção e remediação;

3.128. Reputação do arquivo e correlação da detecção do arquivo em outras soluções de antivírus através de bases de conhecimento como o Vírus Total;

3.129. A solução e as detecções devem apresentar Táticas empregadas baseadas no MITRE ATT&CK

3.130. Resultado da análise do arquivo suspeito pela funcionalidade de Machinne Learning;

3.131. Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado;

3.132. A solução de EDR deverá ser integrado ao agente de antivírus a ser instalado com um com agente único, em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;

3.133. O gerenciamento da solução de EDR deverá ser feito a partir da mesma console de gerenciamento da solução antivírus;

3.134. Deve fornecer guias de repostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder;

3.135. Deve ser capaz de responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça;

3.136. Deve ser capaz realizar buscas de ameaças em todo o ambiente, sendo capaz de buscar por hash, nome, endereços IP, domínio ou linha de comando;

3.137. Deve ter acesso a recurso de Data Lake que armazene informações críticas de endpoints e servidores, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado;

3.138. Deve possibilizar o agendamento de consultas (queries);

3.139. Deve reter os dados no Data Lake por no mínimo 90 dias.

3.140. Funcionalidade de Controle de aplicações e dispositivos:

3.141. Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede;

3.142. Atualiza automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possa ser liberada ou bloqueada;

3.143. Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;

3.144. Oferecer proteção para chaves de registro e controle de processos;

3.145. Proibir através de política a inicialização de um processo ou aplicativo baseado em nome ou no hash do arquivo;

3.146. Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;

3.147. Deve possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;

3.148. Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;

3.149. Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo;

3.150. As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;

3.151. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

3.152. A gestão desses dispositivos deverá feita diretamente console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de endpoints;

3.153. Permitir a autorização de um dispositivo com no mínimo as seguintes opções:

- Permitir que todos os dispositivos do mesmo modelo;
- Permitir que um único dispositivo com base em seu número de identificação único;
- Permitir o acesso total;
- Permitir acesso somente leitura;

3.154. Permitir ainda o bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.

3.155. Funcionalidade de Proteção e Prevenção a Perda de Dados

3.156. Possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo;

3.157. Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo);

3.158. Possibilitar o bloqueio, somente registrar o evento na Console de administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível;

3.159. Deve possuir listas de CCLs pré-configurados com no mínimo as seguintes identificações:

- Números de cartões de crédito;
- Números de contas bancárias;
- Números de Passaportes;
- Endereços;
- Números de telefone;
- Códigos postais definidas por países como Brasil, França, Inglaterra, Alemanha, EUA, etc;
- Lista de e-mails;
- Informações pessoais, corporativas e financeiras referentes especificamente ao Brasil, como CPF, RG, CNH, CNPJ, dados bancários, etc;

- Suportar adicionar regras próprias de conteúdo com um assistente fornecido para essa finalidade;

3.160. Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo.

3.161. Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação;

3.162. Permitir o controle de dados para no mínimo os seguintes meios:

3.163. Anexado no cliente de e-mail (ao menos Outlook e Outlook Express);

3.164. Anexado no navegador (ao menos IE, Firefox e Chrome);

3.165. Anexado no cliente de mensagens instantâneas (ao menos Skype);

3.166. Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD);

CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE PROTEÇÃO PARA SERVIDORES

3.167. Características básicas do agente de proteção contra malwares:

3.168. A solução deverá ser capaz de proteger servidores contra malwares, arquivos e tráfego de rede malicioso, controle de periféricos, controle de acesso à web, controle de aplicativos em um único agente instalado nos servidores;

3.169. Deve realizar a pré-execução do agente para verificar o comportamento malicioso e detectar malwares desconhecidos;

3.170. O agente host deve buscar algum sinal de malwares ativos e detectar malwares desconhecidos;

3.171. O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;

3.172. A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;

3.173. Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de boot;

3.174. Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados;

3.175. Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);

3.176. Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;

3.177. Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;

3.178. É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs);

3.179. Deve suportar o uso de servidores usados para atualização em cache para diminuir a largura de banda usada nas atualizações;

3.180. Deve possuir integração com as nuvens da Microsoft Azure e Amazon Web Services para identificar as informações dos servidores instanciados nas nuvens;

3.181. Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;

3.182. Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção;

3.183. Deve possuir funcionalidades de tecnologias conhecidas como CWPP – Cloud Workload Protection Plataform, permitindo que seja possível trazer funcionalidades de próxima geração para cargas de trabalho em nuvem, bem como containers, e afins;

3.184. A solução deve no mínimo, utilizar o modelo de sensores para containers, garantindo visibilidade e proteção de, no mínimo, estes tipos de ataques:

- Escalação de privilégios dentro de containers;
- Programas utilizando técnicas de mineração de criptomoedas;
- Detecção de atacantes tentando destruir evidências de ambientes comprometidos (IOC – Indicator of compromise);
- Detecção de funções internas do kernel que estão sendo adulteradas em um host;

3.185. A solução deve também se integrar a tecnologias de CSPM – Cloud Security Posture Management, tendo como objetivo trazer funcionalidades de análises integradas de CWPP e CSPM a fim de melhorar a visibilidade e resposta à incidentes em ambientes de nuvem públicas.

3.186. Funcionalidade de Firewall e Detecção e Proteção de Intrusão (IDS\IPS) com as funcionalidades:

3.187. Possuir proteção contra exploração de buffer overflow;

3.188. Deverá possui atualização periódica de novas assinaturas de ataque;

3.189. Deve prover de funcionalidade avançada de proteção preditiva baseada em inteligência artificial e machine learning, capaz de ajustar automaticamente políticas de segurança com base em comportamentos suspeitos e ameaças emergentes, para que possa reduzir a superfície de ataque ao ativar controles adaptativos de acordo com o contexto do ambiente, sem a necessidade de intervenção manual constante.

3.190. A solução de proteção contra ameaças e demais recursos da solução devem funcionar em Modo de segurança do Windows;

3.191. Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo ou dinamicamente através do nome da aplicação.

3.192. Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;

3.193. Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.

3.194. Ser capaz de aplicar uma análise adicional, inspecionando finamente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como buffer overflow.

3.195. Deve possuir técnicas de proteção, que inclui:

3.196. Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;

3.197. Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificado como um vírus;

3.198. Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;

3.199. Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);

3.200. Verificação de ameaças web avançadas: bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados;

3.201. A solução e as detecções devem apresentar Táticas empregadas baseadas no MITRE ATT&CK

3.202. Funcionalidade de Antivírus e AntiSpyware:

3.203. Proteção em tempo real contra vírus, trojans, worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos.

3.204. Proteção anti-malware deverá ser nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

3.205. As configurações do anti-spyware deverão ser realizadas através da mesma console do antivírus;

3.206. Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto;

3.207. Permitir a varredura das ameaças da maneira manual, agendada e em tempo real nos servidores;

3.208. Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus;

3.209. Capacidade de detectar arquivos através da reputação deles;

3.210. Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção;

3.211. A remoção automática dos danos causados deverá ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante;

3.212. Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;

3.213. Deverá detectar tráfego de rede para comandar e controlar os servidores;

3.214. Proteger arquivos de documento contra-ataques do tipo ransomwares;

3.215. Proteger que o ataque de ransomware seja executado remotamente;

3.216. Permitir o envio de amostras de malwares para a nuvem de inteligência do fabricante;

3.217. Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;

3.218. Antivírus de Web (verificação de sites e downloads contra vírus);

3.219. Controle de acesso a sites por categoria;

3.220. Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Safari, Opera e Chrome), fornecendo controle da Internet independentemente do browser utilizado sem utilizar um plugin, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites.

3.221. O Controle da Web deve controlar o acesso a sites impróprios, com no mínimo 14 categorias de sites inadequados. Deve ainda permitir a criação de lista branca de sites sempre permitidos e lista negra de sites que devem ser bloqueados sempre;

3.222. Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio;

3.223. Capacidade de verificar somente arquivos novos e alterados;

3.224. Funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

3.225. Capacidade de habilitar mensagens de desktop para a Proteção contra Ameaças;

3.226. Capacidade de adicionar exclusão de varredura para arquivos, pastas, processos, sites, aplicativos e tipos de explorações detectadas;

3.227. Funcionalidade de proteção contra ransomwares:

3.228. Deve dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;

3.229. Deve dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares;

3.230. Deve dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação;

3.231. A Solução deve ter a capacidade de reverter automaticamente arquivos afetados por ransomware durante a sua execução em tempo real, através de uma tecnologia proprietária, sem depender de VSS (Volume Shadow Copy);

3.232. Funcionalidade de Controle de aplicações e dispositivos:

3.233. Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede;

3.234. Atualiza automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possa ser liberada ou bloqueada;

3.235. Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;

3.236. Oferecer proteção para chaves de registro e controle de processos;

3.237. Proibir através de política a inicialização de um processo ou aplicativo baseado em nome ou no hash do arquivo;

3.238. Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;

3.239. Deve possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;

3.240. Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;

3.241. Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo;

3.242. As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;

3.243. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

3.244. A gestão desses dispositivos deverá feita diretamente console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de endpoints;

3.245. Permitir a autorização de um dispositivo com no mínimo as seguintes opções:

3.246. Permitir que todos os dispositivos do mesmo modelo;

3.247. Permitir que um único dispositivo com base em seu número de identificação único;

3.248. Permitir o acesso total;

3.249. Permitir acesso somente leitura;

3.250. Permitir ainda o bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.

3.251. Funcionalidade de Proteção e Prevenção a Perda de Dados

3.252. Possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo;

3.253. Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo);

3.254. Possibilitar o bloqueio, somente registrar o evento na Console de administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível;

3.255. Deve possuir listas de CCLs pré-configurados com no mínimo as seguintes identificações:

- Números de cartões de crédito;
- Números de contas bancárias;
- Números de Passaportes;
- Endereços;
- Números de telefone;
- Códigos postais definidas por países como Brasil, França, Inglaterra, Alemanha, EUA, etc;
- Lista de e-mails;
- Informações pessoais, corporativas e financeiras referentes especificamente ao Brasil, como CPF, RG, CNH, CNPJ, dados bancários etc.;

3.256. Suportar adicionar regras próprias de conteúdo com um assistente fornecido para essa finalidade;

3.257. Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo.

3.258. Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação;

3.259. Permitir o controle de dados para no mínimo os seguintes meios:

3.260. Anexado no cliente de e-mail (ao menos Outlook e Outlook Express);

3.261. Anexado no navegador (ao menos IE, Firefox e Chrome);

3.262. Anexado no cliente de mensagens instantâneas (ao menos Skype);

3.263. Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD);

3.264. Solução de Endpoint Detection and Response (EDR)

3.265. A solução deve ter capacidade de implementar técnicas de EDR (Endpoint Detection and Response), possibilitando detecção e investigação nos endpoints com atividades suspeitas;

3.266. Deve ter a capacidade de submeter arquivos identificados em incidentes a uma segunda consulta a nuvem de inteligência do fabricante.

3.267. Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do malware e o ponto final de bloqueio.

3.268. Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:

3.269. Detalhes do Processo, como nome, hash, hora e data da detecção e remediação;

3.270. Reputação do arquivo e correlação da detecção do arquivo em outras soluções de antivírus através de bases de conhecimento como o Vírus Total;

3.271. Resultado da análise do arquivo suspeito pela funcionalidade de Machinne Learning;

3.272. Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado;

3.273. A solução de EDR deverá ser integrado ao agente de antivírus a ser instalado com um com agente único, em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;

3.274. O gerenciamento da solução de EDR deverá ser feito a partir da mesma console de gerenciamento da solução antivírus;

3.275. Deve fornecer guias de repostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder;

3.276. Deve ser capaz de responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça;

3.277. Deve ser capaz realizar buscas de ameaças em todo o ambiente, sendo capaz de buscar por hash, nome, endereços IP, domínio ou linha de comando;

3.278. Deve ter acesso a recurso de Data Lake que armazene informações críticas de endpoints e servidores, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado;

3.279. Deve possibilizar o agendamento de consultas;

3.280. Deve reter os dados no Data Lake por no mínimo 7 dias.

SOLUÇÃO DE EXTENDED DETECTION AND RESPONSE (XDR)

3.281. Deve possuir Data Lake que armazene informações críticas de endpoints e servidores, mas também incorporando dados de outras soluções de segurança como firewalls, e-mail gateways, public cloud e mobile, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado;

3.282. Deve possuir recurso de pesquisa estruturada em banco de dados compatível com SQL, ou similar;

3.283. Deve disponibilizar recurso de pesquisa para comparar os indicadores de comprometimento de várias fontes de dados para identificar rapidamente um ataque suspeito;

3.284. Deve utilizar detecções de ATP e IPS do firewall para investigar endpoints suspeitos;

3.285. Deve disponibilizar pontos de aplicação que permitem a executar ações, como colocar em quarentena um endpoint comprometido, bloquear o tráfego de rede ou remover malware;

3.286. Deve possuir sensores que fornecem telemetria de diferentes aspectos da infraestrutura de TI, capazes de identificar dispositivos não gerenciados e desprotegidos em toda o ambiente da organização;

3.287. Deve possibilitar o agendamento de consultas (queries) cíclicas no Data Lake para identificação de IoCs em execuções antecipadas;

3.288. Deve permitir a integração via APIs com sistemas e fluxos de trabalhos já existentes;

3.289. Deve reter os dados no Data Lake por no mínimo 30 dias.

3.290. O XDR deve permitir integração com sistemas de terceiros, no mínimo, tecnologias como Office 365 e produtos de CSPM para visibilidade e correlação de eventos em ambientes de Cloud como Azure, AWS e Google Cloud;

3.291. A console do XDR deve correlacionar os dados recebidos e armazenados no DataLake e gerar evidências de ataques ou eventos suspeitos existentes dentro do ambiente;

3.292. Tais detecções e evidencias devem conter todos os detalhes do evento, bem como uma análise do próprio fabricante sobre a classificação de risco de tal evento;

3.293. Deve possibilitar também que investigações sejam realizadas a partir destes eventos, coletando dados e executando consultas dentro do Datalake ou nos próprios dispositivos a fim de coletar mais evidências para determinar a realidade do ataque presente na console;

3.294. Deve possuir console para gerenciamento de investigações, podendo adicionar de forma automática ou manual, diversos eventos e detecções encontradas na console;

3.295. A console de gerenciamento de investigações deve permitir atribuir analistas que acompanharão a investigação; Será necessário também que exista uma trilha de auditoria para cada investigação, de tal forma que os administradores da console consigam auditar os detalhes da condução da investigação;

3.296. Deve disponibilizar integração com ferramentas de NDR (Network Detect and Response) do próprio fabricante ou de terceiros.

3.297. Considerando que o ambiente atual da Câmara Municipal de São Caetano do Sul, possuí a tecnologia de Sophos XGS 2100 em produção, a solução deverá ser compatível e incluir sem custo integrações com essa plataforma operacional de Firewall.

3.298. As integrações de terceiros poderão ser via API ou envio de Syslogs

3.299. Para integrações, a CONTRATANTE deve fornecer ambiente virtualizado (Microsoft Hyper-V) para instalação de appliance virtual a ser instalado nas dependências da CONTRATANTE.

3.300. A solução deve fornecer ferramenta para a coleta de telemetria de eventos de terceiros que não usam API entregando uma imagem de sistema do tipo .OVA para uso em virtualizador;

3.301. O fabricante deve disponibilizar através de um website a lista de tecnologias e fabricantes suportados, para eventuais consultas;

3.302. Serviço de Detecção e resposta de incidentes - MDR

3.303. O serviço deve ser fornecido e administrado pela CONTRATADA em conjunto do FABRICANTE da solução de proteção de endpoint e servidores ofertada, utilizando-se da ferramenta de monitoramento proativo e resposta gerenciada.

3.304. O fabricante da solução ofertada deve possuir no mínimo as seguintes certificações:

- SOC2 Type II
- ISO 27001:2022
- PCI DSS
- HIPAA Type 2

3.305. A CONTRATADA deverá prover serviço de busca, detecção e resposta a ameaças avançadas do fabricante utilizando-se da solução ofertada;

3.306. Este serviço deve ter funcionamento 24x7x365 e deve contar com time de especialistas do Fabricante da solução de segurança ofertada;

3.307. A ferramenta deve possuir equipes especializadas em no mínimo de 5 SOC's separados geograficamente a fim de manter redundância do serviço;

3.308. Deve prover relatórios com resumos das atividades e incidentes de segurança encontrados no ambiente da CONTRATANTE;

3.309. Deve prover a verificação da integridade dos componentes da solução de segurança instalada no ambiente da CONTRATANTE;

3.310. A solução deverá coletar dados de segurança de várias fontes;

3.311. Deverá trabalhar com Ferramentas de segurança e serviços de resposta de maneira integrada;

3.312. Deve operar sem a necessidade de substituir as ferramentas de segurança existentes;

3.313. O Serviço poderá ser fornecido usando ferramentas integradas do fabricante, ferramentas de terceiros ou a combinação dos dois;

3.314. Deve proporcionar níveis de serviço personalizados, desde notificação detalhada até resposta a incidentes em grande escala;

3.315. Deve disponibilizar integração com ferramentas de NDR (Network Detect and Response) do próprio fabricante ou de terceiros.

3.316. Considerando que o ambiente atual da Câmara Municipal de São Caetano do Sul, possuí a tecnologia de Sophos XGS 2100 em produção, a solução deverá ser compatível e incluir sem custo integrações com essa plataforma operacional de Firewall.

3.317. As integrações de terceiros poderão ser via API ou envio de Syslogs

3.318. Para integrações, a CONTRATANTE deve fornecer ambiente virtualizado (VM Ware ESxi ou Microsoft Hyper-V) para instalação de appliance virtual a ser instalado nas dependências da CONTRATANTE.

3.319. As especificações mínimas para o appliance virtual são:

3.320. Deve rodar em Microsoft Hyper-V;

3.321. A solução deve fornecer ferramenta para a coleta de telemetria de eventos de terceiros que não usam API entregando uma imagem de sistema do tipo .OVA para uso em virtualizador;

3.322. O fabricante deve disponibilizar através de um website a lista de tecnologias e fabricantes suportados, para eventuais consultas;

3.323. O serviço de Monitoramento proativo e resposta gerenciada deverá prover á CONTRATANTE:

3.324. Notificações sobre detecções e detalhes das ameaças encontradas no ambiente;

3.325. Mitigação de incidentes relacionados a ameaças nos dispositivos cobertos com a solução fazendo a contenção de ameaças: os ataques devem ser interrompidos, evitando a propagação;

3.326. Análise de causa raiz realizada para evitar recorrências futuras;

3.327. Canais de comunicação com os especialistas do Fabricante para sanar dúvidas, dar respostas á incidentes e autorizar mudanças e ações preventivas no ambiente computacional da CONTRATANTE;

3.328. A equipe da ferramenta de monitoramento proativo e resposta gerenciada pode utilizar ferramentas de acesso remoto para acessar ou fazer alterações em Endpoints Gerenciados e pode utilizar acesso administrativo ao ambiente da CONTRATANTE para visualizar ou modificar configurações.

3.329. A ferramenta deve possuir equipe de Threat Hunting. Esta equipe será responsável por conduzir o Threat Hunting a fim de buscar proativamente por ameaças que possam ter evitado os controles de detecção existentes com base em inteligência de ameaças e indicadores relevantes de comprometimento observados em engajamentos de Resposta a Incidentes e Investigações.

3.330. O Threat Hunting deve se limitar aos dados coletados do Endpoints Gerenciados e deverá ser focado na identificação de comportamentos e táticas de atacantes. Se o Threat Hunting revelar indicadores de atividade maliciosa, um Caso deverá criado e uma Investigação deve realizada.

3.331. A solução ofertada deve oferecer seguro para ataques cibernéticos bem-sucedidos na infraestrutura monitorada cobrindo despesas incorridas de pelo menos 2 (dois) milhões de reais, incluindo notificação de violação de dados, relações públicas, despesas legais e de conformidade.

3.332. A solução deve oferecer retenção de 1 ano dos dados armazenados;

3.333. A CONTRATANTE reconhece que deve fornecer acesso para a equipe da CONTRATADA para realizar alterações que melhorem a maturidade de segurança dela. A falta de concessão de autorização para tais alterações pode resultar em atividade maliciosa ou na degradação da segurança do ambiente. A CONTRATANTE assume os riscos por quaisquer danos decorrentes ou relacionados a essa nova atividade maliciosa caso haja negativa sobre o pedido da CONTRATADA para autorização para fazer alterações ou modificações.

3.334. A CONTRATANTE reconhece que deve atender a todos os requisitos do item acima, sob pena de perca do seguro disposto.

RELATÓRIOS

3.335. Periodicamente, a CONTRATADA deverá fornecer a CONTRATANTE: (a) relatórios relacionados a Detecções, Casos e Ações de Resposta, e (b) notificação de problemas de Saúde ou configurações significativas incorretas que possam degradar a proteção em tempo real, investigação ou capacidade de tomar Ações de Resposta.

3.336. A solução deve disponibilizar relatórios semanais e mensais sobre o ambiente monitorado.

3.337. O relatório deve conter no mínimo:

3.338. Uma avaliação do nível de proteção do ambiente monitorado, que pode variar entre verde (para um ambiente em compliance), amarelo (para um ambiente na qual os ativos necessitam de atenção e configuração), ou vermelho (na qual o ambiente possui vários ativos com alto risco que precisam de ação imediata);

3.339. Quantidade total de dispositivos licenciados;

3.340. Pipeline de eventos a fim de demonstrar o fluxo de eventos dos ativos integrados;

3.341. Linha de tendência que demonstrando o tipo de casos e de qual fonte sua fonte de detecção;

3.342. Deve ser possível identificar os casos por status: Novo, em progresso, Ação requerida e resolvidos/fechados e demonstrar os números em gráficos.

3.343. Deve demonstrar os tipos de ataque identificados. Por exemplo: Phishing, execução do PowerShell e persistência.

3.344. Deve ser possível identificar o número de detecções por integração, ex.: Endpoints, Firewall.

3.345. Resposta para incidentes deverá ter as seguintes ações.

3.346. A Resposta a Ameaças deve incluir contenção e interrupção de ameaças, e isolamento de endpoint nos dispositivos gerenciados.

3.347. A análise e resposta a incidente devem estar baseadas no ciclo OODA (Observar, Orientar, Decidir, Agir).

3.348. Durante a fase de observação, os analistas devem selecionar pontos-chave de dados que ajudem a estabelecer uma narrativa lógica da atividade, onde cada ponto de dados escolhido tem o potencial de indicar uma atividade maliciosa.

3.349. Durante a fase de Orientação, os analistas devem validar suas observações aplicando os pontos de dados à Matriz MITRE ATT&CK, à Cadeia de Ataques Cibernéticos (Cyber Kill Chain). Se validados os indicadores, a atividade criará uma narrativa de ataque.

3.350. Durante a fase de decisão o analista irá analisar todos os dados coletados e decidirá se há indícios de comprometimento.

3.351. Durante a fase de ação o analista tomará as medidas necessárias com base na conclusão da investigação.

3.352. Caso ocorra qualquer incidente ativo, a equipe de Operações de deverá oferecer suporte direto por chamada, atribui um líder dedicado de resposta a incidentes e garantir que as ameaças sejam totalmente eliminadas.

3.353. Deve ser realizada a investigação de causa raiz para ajudar a prevenir futuros ataques.

3.354. Deve ser possível abrir um incidente por telefone, e-mail;

3.355. No caso de um incidente de segurança no ambiente monitorado, a CONTRATADA através do serviço de Monitoramento proativo e resposta gerenciada deve:

3.356. Atribuir um Líder de Resposta a Incidentes dedicado (um atribuído por turno) para interagir com a CONTRATANTE;

3.357. Realizar a triagem e Investigação para identificar o escopo e o impacto do Incidente para suportar a contenção;

3.358. Analisar as fontes de dados adicionais e dados fornecidos ou disponibilizados pela CONTRATANTE;

3.359. Deverão ser tomadas Ações de Resposta para neutralizar o acesso malicioso e interromper danos adicionais aos ativos ou dados comprometidos;

3.360. Deve ser fornecida a orientação de remediação para a CONTRATANTE quando a Equipe de Serviços de Segurança da CONTRATADA não puder realizar Ações de Resposta no ambiente;

3.361. Devem ser fornecidos relatórios de status do Incidente e rastreamento de itens de ação;

3.362. Deve ser fornecidas recomendações proativas projetadas para prevenir ou reduzir a recorrência do Incidente;

3.363. A CONTRATANTE deve ter acesso direto por chamada à Equipe de Serviços de Segurança para revisar Casos e Incidentes.

4. SUPORTE TÉCNICO E MONITORAMENTO

4.1. Suporte técnico especializado para switches core em alta disponibilidade, incluindo monitoramento, suporte remoto, resposta a incidentes, manutenção preventiva e garantia de continuidade operacional da rede.

4.2. O suporte técnico deverá ser prestado em regime 24x7 (vinte e quatro horas por dia, sete dias por semana) pela própria fornecedora da solução, não sendo permitida subcontratação. O atendimento deverá abranger toda a solução fornecida, incluindo os switches e o software de gerenciamento associado.

4.3. A contratada deverá monitorar o ambiente 24x7 (vinte e quatro horas por dia, sete dias por semana) e todas as soluções descritas neste documento; para toda a estrutura contratada, co ntemplando todo o escopo.

4.4. A CONTRATADA deverá disponibilizar o atendimento de suporte técnico presencial, onde o equipamento que estiver em posso do profissional da CONTRATADA deverá possuir as seguintes soluções de segurança como:

4.5. Chamados e atendimento técnico:

- Antivírus;
- Ferramenta de gestão de acesso privilegiado;
- Criptografia para proteger o ambiente computacional.

4.6. A CONTRATANTE deverá poder abrir chamados de manutenção por meio de ligação telefônica para número com DDD (11), central de atendimento via navegador (Web), WhatsApp da central de atendimento ou correio eletrônico, sem a necessidade de consulta prévia ou qualquer tipo de liberação por parte da fornecedora da solução.

4.7. O atendimento técnico remoto deverá ocorrer 24x7 (vinte e quatro horas por dia, sete dias por semana)

4.8. Não deve haver limites para aberturas de chamados, sejam dúvidas, configurações ou resolução de problemas.

4.9. A equipe de suporte técnico deverá buscar, no escopo de serviços, prevenir a ocorrência de problemas e seus incidentes resultantes, eliminando incidentes recorrentes correlacionando-os e identificando a causa-raiz e sua solução, além de minimizar o impacto dos incidentes que não podem ser prevenidos.

4.10. A fornecedora da solução deverá realizar atendimentos remotos à equipe técnica da CONTRATANTE. Quando o especialista identificar a necessidade de atendimento presencial, este deverá ser previamente alinhado com a equipe da CONTRATANTE. As solicitações poderão ser realizadas pelos analistas ou pelo gestor do processo por meio do sistema de atendimento, telefone ou correio eletrônico.

4.11. Todos os atendimentos deverão estar registrados em central de atendimento técnico e gestão de chamados.

4.12. Deve haver realização de otimizações nas configurações para melhor do desempenho, qua ndo observadas quedas de desempenho ou indisponibilidades pela CONTRATADA

4.13. Garantia de tempo de resposta e nível de serviço;

4.14. A garantia de tempo de resposta será realizada conforme critérios de prioridades a seguir:

Classe	Descrição	Atendimento em até:
1	Serviço indisponível	30 minutos
2	Suporte técnico de maior impacto	1 hora
3	Suporte técnico com menor impacto	4 horas
4	Manutenção preventiva.	A cada 30 dias

4.15. O acordo de nível de serviço para suporte técnico deverá obedecer ao seguinte escopo:

Prioridade	Descrição
1	(Emergencial) O serviço está fora de operação ou há um impacto crítico nas operações dos negócios.
2	(Alta) O serviço está degradado, ou aspectos significativos das operações de negócio sofreram impactos negativos pelo desempenho inadequado.
3	(Média) Serviço funcionando com pequenos problemas sem impacto direto na operação.
4	(Baixa) O desempenho operacional do serviço está prejudicado, não causando quebra de funci onamento ou de operação

4.16. As horas para primeiro atendimento e resolução de incidentes são horas úteis e serão contabilizadas dentro do horário de atendimento descrito neste termo de referência.

4.17. O serviço de monitoramento deverá ser composto de tecnologia que seja totalmente apartada do ambiente computacional e de servidores da CONTRATANTE.

4.18. A CONTRATADA deverá disponibilizar um switch de 8 portas ou superior, para configurar as conexões de rede necessárias para o monitoramento do ambiente sem a necessidade de utilizar os switches da CONTRATANTE.

4.19. O switch deverá conter no mínimo os seguintes recursos:

4.20. Capacidade de comutação: 20 Gbps.

4.21. Tabela de endereços MAC no mínimo de: 8.000 mil.

4.22. Memória interna de no mínimo: 512 MB.

4.23. Memória Flash mínima de: 256MB

4.24. Buffer de pacote mínimo de: 1.5 MB.

4.25. Suportar até 256 VLANS simultaneamente e 4.000 mil Ids de VLAN.

4.26. Interface das 8 portas em 10/100/1000 BASE-T ou superior.

4.27. SFP de 1GB no mínimo de: 2 Interfaces.

4.28. Deverá ser 110w.

4.29. LEDs para representar o status da localidade frontal do hardware.

4.30. A CONTRATANTE não vai disponibilizar hardware ou software para que a CONTRATADA realize o monitoramento.

4.31. A CONTRATADA deverá disponibilizar um recurso tecnológico para que seja o responsável pelo monitoramento e seus sensores.

4.32. O recurso tecnológico deverá ser um dispositivo para monitoramento de toda a infraestrutura CONTRATADA pela CONTRATANTE conforme os itens destacados neste termo de referência.

4.33. A fonte de carregamento e gerenciamento de energia deverá ser conectada através da porta tipo-C.

4.34. A CONTRATANTE não disponibilizará recursos computacionais para a instalação do sistema de monitoramento.

4.35. O recurso tecnológico poderá consumir até uma tomada do rack com o tipo padrão NBR 14136 de três pinos.

4.36. O recuso tecnológico deverá ser acompanhado com uma fonte de 100/240 VA, padrão NBR 14136 de três pinos, com botão que tenha a possibilidade de ligar e desligar o recurso energético da fonte, deverá entregar 5V de 3000mA e o fio de conexão com a fonte de energia não deverá ser superior a 100cm.

4.37. O tamanho do recurso tecnológico deverá ter não menos do que 9 cm de largura, 3 cm de altura e 6 cm de profundidade.

4.38. O tamanho do recurso tecnológico não deverá ser superior a 10 cm de largura, 3,5 cm de altura e 7 cm de profundidade.

4.39. Deverá possuir uma entrada do tipo RJ-45 com a velocidade de Gigabite 10/100/1000.

4.40. Deverá possuir 2 entradas USB 2.0.

4.41. Deverá possuir 2 entradas de USB 3.0.

4.42. Deverá possuir 2 entradas Micro HDMI 2.0.

4.43. A entrada Micro HDMI deverá possuir o suporte de resolução em 4Kp60.

4.44. Deverá possuir uma entrada A/V habilitado para TV out.

4.45. Deverá possuir 1 entrada categorizada como tipo-C.

4.46. O recurso tecnológico de monitoramento deverá ter suporte para sistema operacional Linux.

4.47. A comunicação com o datacenter deverá ser feita através do protocolo de comunicação TCP.

4.48. O recurso tecnológico deverá possuir um cooler para que ele consiga realizar a dissipação de calor assim evitando qualquer tipo de impacto no serviço de monitoramento.

4.49. O recurso tecnológico deverá possuir furação para que a dissipação de calor seja mais eficiente;

4.50. O recurso tecnológico deverá possuir o armazenamento em MicroSD de no mínimo 64gb;

4.51. A CONTRATADA ficará responsável em realizar a entrega do recurso tecnológico juntamente com as respectivas licenças do sistema operacional e softwares de segurança como licença contra-ataques cibernéticos, backup do sistema operacional e até mesmo monitoramento do sistema tecnológico.

4.52. O serviço de switches em alta disponibilidade deverá ter disponível API's de comunicação para integração com inteligência artificial voltada a cibersegurança.

4.53. A inteligência artificial deverá atender todos a estrutura de switches core e ter compatibilidade com a estrutura ATIVO/PASSIVO.

4.54. A inteligência artificial deverá monitorar todas as ações e regras configuradas no cluster de switches para levantamento dos dados referentes as configurações executadas medindo o seu nível de efetividade.

4.55. Integrar-se aos sistemas de logs dos switches para coletar, analisar e correlacionar eventos.

4.56. A criação de logs deverá ser em tempo real.

4.57. Atuar como uma plataforma centralizada para gerenciar várias com visibilidade da topologia do cluster, oferecendo visibilidade de toda a infraestrutura de segurança.

4.58. Em resposta a eventos ou ameaças detectadas, a solução pode disparar ações automáticas, como bloqueio de IPs, isolamento de dispositivos, ou alterações nas regras de firewall para mitigar riscos.

4.59. Deverá ajudar a configurar e gerenciar as políticas de segurança no firewall, permitindo ajustes em tempo real de acordo com as necessidades da organização.

4.60. Através da integração com os switches, a solução deverá oferecer um painel de monitoramento em tempo real, com relatórios detalhados sobre o tráfego de rede, ataques detectados e atividades suspeitas.

4.61. Deverá identificar vulnerabilidades de segurança em dispositivos na rede e sugerir ou aplicar correções baseadas nas configurações do firewall.

4.62. Quando integrada com a os switches deverá entregar uma abordagem de segurança mais robusta, correlacionando eventos e tomando medidas mais eficazes para a proteção da rede em tempo real.

4.63. Integração com as funcionalidades de prevenção de intrusões (IPS) e proteção contra malware, para uma resposta rápida a ameaças emergentes.

4.64. A inteligência artificial deve ter a capacidade de fazer controle de acesso baseado em funções (RBAC), permitindo determinar qual função tem permissão para acessar determinados agentes.

4.65. A inteligência artificial deve ter a capacidade de fazer controle de acesso baseado em atributos (ABAC), permitindo determinar permissão das funções no mínimo nos seguintes atributos, recursos de contexto, endpoints e chat.

4.66. A inteligência artificial deve ser capaz de tomas ações através dos agentes por SSH ou API, sem a necessidade de utilizar softwares de terceiros.

4.67. A inteligência artificial deve permitir a instrução específica por ativos.

4.68. A inteligência artificial deve permitir que o agente instalado em endpoint com sistemas operacionais Windows (10, 11, Server 2016, 2019, 2022.), Linux (Ubuntu (18.04+), CentOS/RHEL (7+), Debian, Fedora) e MacOS (11 Big Sur ou mais recentes), funcionem no modo agente ou coletor.

4.69. A inteligência artificial deve permitir que o agente no modo coletor instalado em endpoints, possam se integrar a outros equipamentos ou sistemas de tecnologia.

4.70. A CONTRATADA deverá monitorar o ambiente 24x7 (vinte e quatro horas por dia, sete dias por semana) descrito nesse documento;

4.71. O monitoramento deverá ter vigência de 24 (vinte e quatro) meses;

4.72. A disponibilidade e monitoramento deverá ocorrer por 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana;

4.73. O ambiente de monitoramento deverá ser hospedado em ambiente de alta disponibilidade.

4.74. Deverá ter SLA de disponibilidade da console de gerenciamento de no mínimo 99,98%;

4.75. A solução de monitoramento deverá estar hospedada em datacenter com a classificação mínima de Tier III;

4.76. A solução de monitoramento deverá ter portal de acesso de visualização WEB disponibilizada para a CONTRATANTE;

4.77. Deverá ser capaz de enviar alertas de alteração de status de sensores através de correio eletrônico;

4.78. Possuir pelo menos os seguintes status para os sensores de monitoramento: Estado normal, estado de alerta e estado de erro;

4.79. Possuir a possibilidade para criação de interface WEB com mapa de distribuição de arquitetura com o monitoramento, podendo ter acesso público e/ou autenticado através de contas de usuários internas da solução de monitoramento;

4.80. O monitoramento deverá ser compatível com os principais serviços de nuvem pública;

4.81. O sistema de monitoramento deverá contar com aplicativo de administração instalável e homologado para o sistema operacional Linux;

4.82. A solução de monitoramento deverá abrir chamado de maneira automática junto a CONTRATANTE, após a alteração de um sensor para o estado de alerta ou erro;

4.83. A ferramenta de monitoramento deve ser capaz de realizar a coleta de dados de diversos dispositivos e sistemas, incluindo servidores, dispositivos de rede e aplicações. Os principais requisitos incluem:

4.84. A ferramenta deverá realizar a coleta de métricas de desempenho, como uso de CPU, memória, espaço em disco, latência de rede, e status de serviços. A coleta será feita de forma

agendada ou por meio de eventos de trap (alerta gerado pelo próprio dispositivo) onde será necessário que os dispositivos entreguem as informações através do protocolo SNMP.

4.85. A ferramenta deverá ser capaz de monitorar diversos tipos de hosts, com a possibilidade de utilização de agentes para coleta de dados, bem como monitoramento sem agentes para dispositivos de rede e outros dispositivos que não possuam um agente instalado.

4.86. A ferramenta deve ser capaz de gerar alertas e notificações de forma automatizada, baseados em eventos ou métricas predefinidas. As notificações poderão ser enviadas por e-mail ou outras integrações, como sistemas de gerenciamento de incidentes. A ferramenta deverá também permitir a definição de escalonamentos de alertas e ações automáticas, como reiniciar um serviço ou executar comandos específicos em resposta a incidentes quando houver a disponibilidade de conexão via SSH.

4.87. A ferramenta deverá possuir uma interface gráfica baseada na web que permita a visualização de dados em tempo real, com dashboards personalizáveis. A interface deve ser intuitiva, acessível e permitir a criação de relatórios gerenciais com informações detalhadas sobre a saúde e o desempenho da infraestrutura.

4.88. A plataforma deverá garantir segurança através de autenticação de usuários e controle de permissões, permitindo a definição de diferentes níveis de acesso. A comunicação entre a ferramenta e os dispositivos monitorados deverá ser criptografada para garantir a proteção dos dados durante a transmissão.

4.89. A solução deverá ser escalável, permitindo seu uso tanto em ambientes de pequeno porte quanto em grandes infraestruturas corporativas, com a possibilidade de monitoramento de milhares de dispositivos simultaneamente. Para grandes ambientes, deverá ser possível utilizar proxies para distribuição do monitoramento.

4.90. A ferramenta deve permitir a geração de relatórios periódicos, tais como dia anterior, semana anterior, mês anterior, ano anterior e a realização de análises de tendências para prever possíveis falhas ou pontos de saturação da infraestrutura. A análise histórica deverá ser capaz de identificar padrões e comportamentos anormais através do armazenamento dos históricos no recurso tecnológico que a CONTRATADA deverá entregar com o serviço de monitoramento.

4.91. A ferramenta deve ser compatível com sistemas operacionais Linux e Windows, e permitir a instalação em ambientes físicos ou virtuais, de acordo com a necessidade do cliente.

4.92. A ferramenta deverá utilizar uma base de dados para armazenar as informações coletadas, com a possibilidade de utilização de bancos de dados open-source, como MySQL, PostgreSQL ou similares.

4.93. A solução deverá permitir integrações com outras plataformas de TI, como sistemas de gerenciamento de incidentes, plataformas de visualização de dados, e outras ferramentas de automação e análise de infraestrutura.

4.94. A implementação da ferramenta será realizada em etapas, incluindo a instalação do proxy através do recurso tecnológico, configuração e personalização conforme os requisitos específicos da infraestrutura de TI.

4.95. Deverá ser possível a geração de relatórios com dados de tabela e gráficos para quaisquer sensores que compõem a solução;

RELÁTORIOS

4.96. Deverá ser fornecido relatórios mensais de chamados e monitoramento de recursos dos componentes do serviço, com:

4.97. Relatório de Chamados (referente ao serviço descrito nesse lote):

- Categoria do chamado;
- Usuário;
- Ativos relacionados;
- Data de abertura e fechamento;
- Status;

4.98. Relatório de Monitoramento de recursos (referente ao serviço descrito nesse lote):

4.99. Disponibilidade;

4.100. Consumo de hardware (CPU, memória, disco, consumo de banda);

4.101. Alertas e erros;

5. SERVIÇO DE INSTALAÇÃO

5.1. É responsabilidade da CONTRATADA definir projeto de implantação, com atividades, cronograma e dimensionamento de recursos, de forma a atender os requisitos de nível de serviço e prazos estabelecidos na Especificação dos Serviços.

5.2. A empresa CONTRATADA fornecerá um serviço de onboarding para a tecnologia onde trabalhará com o CONTRATANTE para integrar a solução e suportar a configuração e integração corretas das fontes, incluindo as seguintes:

5.3. A CONTRATADA fornecerá documentação arquitetónica que identifica os pontos de conexão entre a solução ofertada, o ambiente do CONTRATANTE e o ambiente de serviço.

5.4. A CONTRATADA coordenará todas as responsabilidades, tarefas e relatórios de status de CONTRATANTE relacionados à entrega do recurso, e orientará e ajudará CONTRATANTE na transição para co-gerenciar a Tecnologia Contratada.

5.5. A fase de onboarding deve seguir pelo menos estas fases com os seguintes requisitos mínimos:

- Kick-off call: Alinhamento de objetivos e expectativas, alinhamento do onboard e da jornada. Alinhamento das integrações e configurações necessárias. Defininição de próximos passos.
- Serviço de Implementação e Configuração: Definição de melhores práticas de Configuração, configuração de Integração com as ferramentas definidas, Treinamento, implantação em ambiente e avaliação de postura de Segurança.
- Workshop de demonstração de funcionalidades: Serviços e termos de engajamento, definição de fatores de sucesso, introdução a ferramenta e definição de pontos focais de contato
- Revisão de Serviços: Relatórios de resultados da implementação, verificação de ferramenta implementada.

5.6. A CONTRATADA em conjunto com a CONTRATANTE realizará todas as atividades necessárias durante o processo de integração.

5.7. A CONTRATANTE deve: a) ter uma conta para visualização do portal da ferramenta de Serviço de Monitoramento proativo e resposta gerenciada válida e ativa, b) implantar e configurar o Software de Serviço aplicável em Endpoints Gerenciados, c) manter conformidade com todos os requisitos identificados nas Verificações de Saúde, e d) atender aos requisitos mínimos do sistema para instalar o Software de Serviço, e) configurar todos os Sistemas de Terceiros necessários para permitir a transmissão de toda a telemetria de segurança aplicável em um formato compatível com o Serviço; e f) executar apenas versões suportadas do Software de Serviço e/ou ferramentas de segurança de terceiros.

5.8. A CONTRATANTE reconhece e concorda que o Software de Serviço deve ser implantado em pelo menos oitenta por cento (80%) do volume licenciado, pois isso é necessário para fornecer à Equipe de Serviços de Segurança uma visibilidade suficiente no ambiente da CONTRATANTE para a entrega do Serviço. A CONTRATADA não será responsável ou responsabilizada por quaisquer problemas causados pela falha da CONTRATANTE em configurar ou habilitar as configurações de segurança disponibilizadas pela equipe da CONTRATADA ou por quaisquer problemas causados pela falha da CONTRATANTE em cumprir quaisquer requisitos aplicáveis.

5.9. A CONTRATANTE deve fazer esforços razoáveis para remediar prontamente quaisquer comprometimentos relatados pelo Serviço de Monitoramento proativo e resposta gerenciada. A CONTRATADA não será responsável ou responsabilizada por quaisquer problemas causados pela falha da CONTRATANTE em tomar medidas de remediação de forma oportuna.

5.10. A Equipe de Serviços de Segurança não tem obrigação de notificar a CONTRATANTE ou gerar novos Casos a partir de Detecções para as quais a CONTRATADA já forneceu etapas de remediação recomendadas.

5.11. Deverão ser instalados e configurados os itens físicos e lógicos seguindo os padrões e melhores práticas recomendadas na norma NBR ISO/IEC 27002 e conforme critérios definidos pela contratante;

5.12. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às normas legais e regulamentares aplicáveis e às recomendações aceitas pela boa técnica;

5.13. Prestar todos os esclarecimentos que lhe forem solicitados, atendendo prontamente a quaisquer reclamações;

5.14. Fornece toda mão de obra necessária à completa execução do serviço, bem como ferramentas e equipamentos a serem utilizados na manutenção e reparos;

5.15. Instalação física de todos os equipamentos em Rack disponibilizado no local de instalação;

5.16. Os equipamentos devem ser configurados em alta disponibilidade, no modo ativo/ativo ou ativo/passivo, dois equipamentos funcionando simultaneamente e em caso de falha o outro continue em operação;

5.17. Os profissionais alocados para a instalação por parte da contratada deverão ter conhecimento pleno nas melhores práticas de configuração do produto e fabricantes;

5.18. Os profissionais técnicos quando em serviço na Câmara Municipal de São Caetano deverão apresentar documento de identificação com foto e identificação da empresa com os seguintes: RG/CNH;

5.19. Estar devidamente uniformizado para identificação da CONTRATADA.

5.20. A contratante deverá designar um profissional para acompanhar o processo de implementação, com a finalidade de esclarecimentos sobre o ambiente.

5.21. Juntamente com a proposta deverá ser apresentada documentação oficial do fabricante contendo as especificações técnicas dos produtos ofertados para verificação do responsável pela análise técnica.

CÂMARA MUNICIPAL DE
SÃO CAETANO DO SUL

MODELO DE PROPOSTA COMERCIAL

Nome da Empresa:		
E-mail		
Endereço:	**Nº**	**Bairro:**
Cidade:	**Estado:**	**CEP:**
CNPJ Nº:	**Inscrição Estadual:**	**Fone:**

LOTE ÚNICO				
ITEM	**DESCRIÇÃO**	**QTDE MESES**	**VALOR UNITÁRIO**	**VALOR TOTAL**
1	SERVIÇO ESPECIALIZADO DE SWITCHES CORE	24		
2	PLATAFORMA DE GESTÃO E CONECTIVIDADE PARA WI-FI	24		
3	SERVIÇO DE SEGURANÇA CIBERNÉTICA	24		
4	SUPORTE TÉCNICO E MONITORAMENTO	24		
5	SERVIÇO DE INSTALAÇÃO	1		
VALOR GLOBAL 24 MESES				

Declaramos expressamente, sob as penas da Lei que:

1) Esta empresa está em situação regular perante o Ministério do Trabalho, uma vez que cumpre as disposições impostas pelo inciso XXXIII, do Artigo 7º, da Constituição Federal;

2) A proposta econômica apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega da proposta.

3) Atende à reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991.

Validade da Proposta: 60 DIAS

Local de entrega: Avenida Goiás, nº 600 – Centro – São Caetano do Sul – SP

CÂMARA MUNICIPAL DE
SÃO CAETANO DO SUL

Local: _____, _____/_____/2026.

Nome do Responsável: _____

_____

Assinatura do Representante da Empresa