ESTUDO TÉCNICO PRELIMINAR – ETP

1. NECESSIDADE DA CONTRATAÇÃO

1.1. A necessidade de contratação de uma empresa especializada para fornecer appliances de firewall de próxima geração (NGFW) com redundância, e licenças de software antivírus com recursos XDR, é justificada pela crescente demanda de proteção contra ameaças cibernéticas sofisticadas e pela necessidade de garantir a segurança das informações, além de assegurar a continuidade das operações digitais na Câmara Municipal de Itanhaém. Abaixo estão os principais motivos que tornam essa contratação imprescindível:

1.1.1. O ambiente digital está cada vez mais exposto a ameaças cibernéticas avançadas, como ransomware, phishing, ataques direcionados e malwares persistentes. A Câmara, por lidar com informações confidenciais, tanto de servidores quanto de cidadãos, precisa de uma solução de segurança robusta que ofereça proteção em tempo real contra ataques complexos, combinando NGFW e software antivírus com recursos XDR.

1.1.2. O NGFW oferece inspeção profunda de pacotes (DPI), controle de aplicativos e proteção contra intrusões, garantindo a segurança da rede em todas as suas camadas.

1.1.3. O XDR (Extended Detection and Response) integra diferentes vetores de dados (rede, endpoints, servidores) para fornecer uma visão unificada das ameaças, permitindo uma resposta mais rápida e coordenada em caso de ataques.

1.1.4. A continuidade dos serviços é essencial para a Câmara. A redundância no sistema de firewall garante que, em caso de falha de um equipamento, outro assuma automaticamente, evitando interrupções nos serviços críticos e assegurando o funcionamento ininterrupto da infraestrutura de TI.

1.1.5. A Lei Geral de Proteção de Dados (LGPD) exige que todas as instituições públicas adotem medidas adequadas para garantir a segurança das informações pessoais sob sua custódia. A contratação de um NGFW com XDR assegura conformidade com as melhores práticas de segurança e regulamentações, prevenindo vazamentos e acessos não autorizados.

1.1.6. A contratação de appliances de firewall de próxima geração com redundância e licenças de software antivírus com recursos XDR é uma necessidade estratégica para proteger as operações e informações digitais da Câmara Municipal de Itanhaém. Além de garantir a continuidade dos serviços, a solução proporcionará conformidade com a legislação, segurança avançada contra ameaças cibernéticas e uma gestão eficiente da infraestrutura de TI, permitindo que a Câmara esteja preparada para os desafios futuros da segurança digital.

1. DEMONSTRAÇÃO DA PREVISÃO DA CONTRATAÇÃO NO PLANO DE CONTRATAÇÕES ANUAL

1.1. O Plano de Contratações para o Exercício 2024 não foi elaborado.

2. REQUISITOS DA CONTRATAÇÃO

2.1. Para garantir a segurança da infraestrutura de TI da Câmara Municipal de Itanhaém, a contratação de uma empresa especializada no fornecimento de appliances de firewall de próxima geração (NGFW) com redundância e licenças de uso de software antivírus com recursos XDR deve atender a uma série de requisitos técnicos, operacionais e legais. Abaixo estão os principais requisitos que devem ser considerados para a contratação:

2.1.1. Requisitos Técnicos:

2.1.1.1. Firewall de Próxima Geração (NGFW):

a) O NGFW deve realizar inspeção profunda de pacotes (Deep Packet Inspection) para detectar e bloquear ameaças avançadas em tempo real.

b) Deve oferecer controle granular de aplicações, permitindo bloquear, priorizar ou limitar o uso de aplicativos específicos.

c) Implementação de um sistema de prevenção de intrusões (IPS) para detectar e impedir tentativas de invasão e exploração de vulnerabilidades.

d) O NGFW deve incluir redundância automática para assegurar a continuidade dos serviços em caso de falhas. Isso inclui suporte a failover, load balancing e alta disponibilidade.

e) Suporte a VPNs seguras (IPsec, SSL VPN) para permitir conexões remotas seguras.

f) Capacidade de suportar um tráfego de rede de alta demanda, com largura de banda mínima suportada conforme as necessidades da Câmara.

2.1.1.2. Software Antivírus com XDR

a) A solução antivírus deve incluir XDR para correlacionar eventos de segurança em vários pontos (endpoint, rede, servidor) e oferecer visibilidade unificada.

b) Monitoramento em tempo real de todos os dispositivos da rede, com detecção automática de ameaças e resposta proativa.

c) Capacidade de detectar e responder a ameaças desconhecidas e persistentes por meio de análise comportamental.

d) O Software Antivírus deve ser totalmente integrável com o NGFW para oferecer uma resposta coordenada e centralizada a incidentes.

e) Ferramentas de automação para executar respostas a ameaças e remediação de incidentes com o mínimo de intervenção manual.

2.1.2. Requisitos Operacionais:

2.1.2.1. O fornecedor deve garantir atualizações automáticas regulares e rápidas para proteção contra novas ameaças emergentes.

2.1.2.2. A empresa contratada deve fornecer suporte técnico 24/7, com tempo de resposta rápido e eficiente para resolução de problemas. Além disso, deve incluir manutenção preventiva e corretiva dos appliances e software.

2.1.2.3. A solução deve ser escalável, permitindo aumento de capacidade e adaptação às necessidades futuras da Câmara, tanto em termos de número de usuários quanto de dispositivos e tráfego.

2.1.2.4. Interface de gerenciamento unificada para monitorar e controlar a segurança da rede, incluindo geração de relatórios detalhados e customizáveis.

2.1.3. Requisitos de Conformidade Legal e Normativa:

2.1.3.1. As soluções devem atender aos requisitos da Lei Geral de Proteção de Dados (LGPD), garantindo a segurança e a privacidade dos dados tratados pela Câmara Municipal.

2.1.3.2. O NGFW e o Software Antivírus devem possuir certificações reconhecidas internacionalmente, como ISO 27001 e NIST, que atestem a robustez de suas medidas de segurança.

2.1.3.3. As soluções devem permitir a criação de logs detalhados e auditorias, facilitando o cumprimento de auditorias internas e exigências regulatórias.

2.1.3.4. A solução deve incluir um plano de resposta a incidentes, alinhado com as melhores práticas do mercado e conforme as regulamentações específicas do setor público.

2.1.4. Requisitos de Sustentabilidade:

2.1.4.1. Os appliances de firewall devem ser certificados por sua eficiência energética, garantindo baixo consumo de energia e contribuindo para a sustentabilidade ambiental.

2.1.4.2. A empresa fornecedora deve oferecer garantias de descarte e substituição adequados dos equipamentos, seguindo as normas de sustentabilidade e evitando desperdícios.

2.1.4.3. O fornecedor deve adotar práticas sustentáveis em seus processos, como redução de emissões de carbono e reutilização de materiais.

2.1.5. Critérios de Qualidade e Desempenho:

2.1.5.1. Garantia de um tempo de resposta baixo para detecção e mitigação de ameaças.

2.1.5.2. Compromisso com alta disponibilidade e uptime de pelo menos 99,9%, assegurando a mínima interrupção nos serviços de TI.

2.1.5.3. A empresa contratada deve oferecer treinamento técnico completo para a equipe de TI da Câmara, garantindo pleno entendimento das funcionalidades e operação do NGFW e do Software Antivírus.

3. ESTIMATIVAS DAS QUANTIDADES PARA A CONTRATAÇÃO

3.1. Abaixo seguem as estimativas de quantidades, levando em consideração a estrutura atual e o crescimento esperado da Câmara Municipal, bem como a necessidade de segurança cibernética robusta e escalável.

3.1.1. Appliances de Firewall de Próxima Geração (NGFW) com Redundância

3.1.1.1. Quantidade de Appliances (Firewall NGFW)

3.1.1.1.1. **Estimativa**: 2 appliances (em modo redundante/alta disponibilidade)

3.1.1.1.2. **Justificativa**: Para garantir alta disponibilidade (HA) e failover automático, um segundo firewall deve ser instalado para prover redundância, de forma que, em caso de falha de um dispositivo, o outro assuma as funções automaticamente, sem interrupção dos serviços.

3.1.1.2. Licenças de Recursos de Segurança Adicionais

3.1.1.2.1. **Estimativa**: 2 licenças (uma para cada appliance)

3.1.1.2.2. **Justificativa**: Licenciamento para funcionalidades avançadas de segurança da Web contra ameaças transmitidas pela Web, incluindo filtragem ATP + DNS, filtragem de URL, filtragem de vídeo e serviços de comunicação anti-botnet, C2, HA (High availability), WAF e controle granular de aplicativos deve ser adquirido para cada appliance.

3.1.1.3. Licenças de Uso de Software Antivírus com Recursos XDR para Desktops e Servidores

3.1.1.3.1. **Desktops**

3.1.1.3.1.1. **Quantidade de Licenças:** 70 licenças

3.1.1.3.1.2. Justificativa: Estimativa baseada no número de desktops em uso pela Câmara Municipal. É recomendável cobrir todos os desktops utilizados por funcionários, incluindo aqueles em áreas administrativas, legislativas e de suporte.

3.1.1.3.2. Servidores

3.1.1.3.2.1. Quantidade de Licenças: 6 licenças

3.1.1.3.2.2. Justificativa: Para servidores críticos que operam serviços e aplicações essenciais, deve-se garantir a proteção adequada. O número de licenças deve considerar servidores de aplicação, de banco de dados e de arquivos.

3.2. Portanto, em relação as licenças necessárias ficam quantificado da seguinte forma:

Item	Descrição	CATSER	UN	Quantidade
1	Appliance de Firewall de Próxima Geração (NGFW)	609340	UN	2
	Licenciamento para funcionalidades avançadas de segurança da Web para proteger as organizações contra ameaças transmitidas pela Web, incluindo filtragem ATP + DNS, filtragem de URL, filtragem de vídeo e serviços de comunicação anti-botnet, C2, HA (High availability), WAF e controle granular de aplicativos deve ser adquirido para cada appliance, por 12 meses.	27502	Licença	2

2	Licença de Uso de Software Antivírus com Recursos XDR para Desktops, por 12 meses.	27502	Licença	70
	Licença de Uso de Software Antivírus com Recursos XDR para Servidor, por 12 meses.	27502	Licença	6

4. LEVANTAMENTO DE MERCADO

4.1. Para garantir uma contratação adequada e economicamente vantajosa, o levantamento de mercado tem como objetivo identificar as principais empresas fornecedoras de soluções de segurança de rede e software antivírus com recursos XDR. Esse levantamento inclui informações sobre fabricantes, preços, características dos produtos e condições de suporte técnico. Abaixo estão os principais aspectos a serem considerados no levantamento.

4.1.1. Fabricantes e Soluções de Appliances de Firewall NGFW:

4.1.1.1. Sophos

4.1.1.1.1. Modelos: Sophos XGS Series (XGS 126, XGS 136)

4.1.1.1.2. Características: Oferece integração com o sistema de Segurança Sincronizada e proteção avançada contra ameaças com IPS, DPI e Sandbox.

4.1.1.1.3. Suporte: Contrato de suporte 24x7 com atualizações automáticas de segurança e firmware.

4.1.1.2. Fortinet

4.1.1.2.1. Modelos: FortiGate (FG-100F, FG-200F)

4.1.1.2.2. Características: Equipado com proteção de rede e SD-WAN integrada para alta performance, escalabilidade e proteção unificada de ameaças com inspeção profunda.

4.1.1.2.3. Suporte: Disponível com pacotes de suporte 24x7 com SLAs rápidos.

4.1.1.3. Palo Alto Networks

4.1.1.3.1. Modelos: **PA-220, PA-820**

4.1.1.3.2. Características: Integração com a plataforma de segurança **PAN-OS**, recursos de **Segurança em Nuvem** e proteção avançada contra ameaças.

4.1.1.3.3. Suporte: Suporte técnico 24x7, com atualização de software e análise de ameaças em tempo real.

4.1.1.4. Cisco (Firepower Series)

4.1.1.4.1. Modelos: **Cisco Firepower 1010, 1120**

4.1.1.4.2. Características: Oferece **proteção contra ameaças avançadas (APT)**, **filtros de URL** e monitoramento em tempo real de tráfego de rede.

4.1.1.4.3. Suporte: Suporte 24x7 com contratos de manutenção e garantia estendida.

4.1.2. Fornecedores de Software Antivírus com Recursos XDR

4.1.2.1. Sophos Intercept X Advanced with XDR

4.1.2.2. Recursos: Integração com o firewall Sophos, proteção de endpoint, e detecção e resposta estendida a ameaças. Inclui monitoramento de rede e automação de respostas a incidentes.

4.1.2.3. Suporte: Suporte técnico 24x7 com monitoramento proativo e assistência na resposta a incidentes.

4.1.2.4. CrowdStrike Falcon XDR

4.1.2.5. Recursos: Fornece proteção avançada para endpoints com análise de inteligência de ameaças, prevenção de malware, e recursos de investigação detalhada de incidentes.

4.1.2.6. Suporte: Suporte 24x7 com análise contínua de ameaças e atualizações automáticas.

4.1.2.7. Microsoft Defender for Endpoint with XDR

4.1.2.8. Recursos: Plataforma integrada que combina segurança na nuvem, gerenciamento de endpoints e proteção contra ransomware e ataques avançados.

4.1.2.9. Suporte: Suporte 24x7 com integração com o Azure e resposta automática a incidentes.

4.1.2.10. SentinelOne Singularity XDR

4.1.2.11. Recursos: Detecção e resposta automatizada com análise de ameaças em tempo real e inteligência de machine learning para prevenção de ataques.

4.1.2.12. Suporte: Suporte técnico 24x7 com respostas rápidas a incidentes e atualizações automáticas.

5. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

5.1. Para a presente solução a ser contratada foi utilizado o seguinte critério:

Consulta com utilização de dados de pesquisa publicada em mídia especializada.

Item	Descrição	CATSER/ CATMAT	UN	Quantidade	Valor Unitário	Valor Total
1	Appliance de Firewall de Próxima Geração (NGFW)	609340 CATMAT	UN	2	R$ 28.000,00	R$ 56.000,00
	SFP+ 10GB (Fibra Multimodo) Transceiver Optico 100% Compatível com Appliance de Firewall fornecido.	18514 CATMAT	UN	4	R$ 1.300,00	R$ 5.200,00
	SFP 1GB (Fibra Multimodo)	18514 CATMAT	UN	4	R$ 760,00	R$ 3.040,00

	Transceiver Optico 100% Compatível com Appliance de Firewall fornecido.					
	Fonte de Alimentação adicional Compatível com Appliance de Firewall fornecido.	7716 CATMAT	UN	2	R$ 1.450,00	R$ 2.900,00
	Licenciamento para suporte técnico avançado e funcionalidades avançadas de segurança do Appliance de Firewall de Próxima Geração (NGFW) fornecido contra ameaças transmitidas pela Web, incluindo filtragem ATP + DNS, filtragem de URL, anti-botnet, C2, HA (High availability), WAF e outros, por 12 meses.	27502 CATSER	Licença	2	R$ 8.000,00	R$ 8.000,00
2	Licença de Uso de Software Antivírus com Recursos XDR para Desktops, por 12 meses.	27502 CATSER	Licença	80	R$ 600,00	R$ 48.000,00

	Licença de Uso de Software Antivírus com Recursos XDR para Servidor, por 12 meses.	27502 CATSER	Licença	6	R$ 1.050,00	R$ 6.300,00

5.2. Por ora, consideraremos uma estimativa preliminar de R$ 129.440,00 (Cento e vinte e três mil quatrocentos e quarenta reais).

6. DESCRIÇÃO DA SOLUÇÃO

6.1. SOLUÇÃO A SER ADOTADA

6.1.1. A solução proposta para a contratação de empresa especializada no fornecimento de appliances de firewall de próxima geração (NGFW) com redundância e licenças de uso de software antivírus com recursos XDR para desktops e servidores é baseada na necessidade de garantir a segurança da infraestrutura de TI, proteção contra ameaças cibernéticas avançadas, e a continuidade operacional. A seguir, detalho os principais componentes dessa solução.

6.1.2. Appliances de Firewall de Próxima Geração (NGFW) com Redundância:

6.1.2.1. Especificações Técnicas Mínimas:

- **Firewall throughput:** até 20 Gbps (Capacidade de Processamento)
- **IPsec VPN Throughput** : 11.5 Gbps
- **IPS Throughput** : 2.6 Gbps
- **NGFW Throughput**: 1.6 Gbps
- **Threat Protection Throughput**: 1 Gbps
- **Firewall Latency**: 4.97µs

- **Concurrent Sessions**: 1.5 Million
- **New Sessions/Sec**: 56.000
- **Firewall Policies**: 10.000
- **SSL VPN Throughput** : 1 Gbps
- **Concurrent SSL VPN Users**: 500
- **SSL Inspection Throughput**: 1 Gbps
- **Application Control Throughput**: 2.2 Gbps
- **Interfaces**: 2x 10 GE SFP+, 18x GE RJ45, 4x Shared Port Pairs, 8x GE SFP
- **Local Storage**: 480 GB
- **Power Supplies**: Dual AC PS
- **Form Factor**: 1 RU

6.1.2.2. Funções Gerais

- A interface gráfica web (GUI) deve oferecer uma maneira intuitiva de configurar, monitorar e gerenciar o firewall.
- Permitir um gerenciamento avançado e direto dos recursos de segurança do firewall através de CLI.
- Permitir a integração com servidores de diretório (como Active Directory) para autenticar usuários, garantindo que as políticas de segurança sejam aplicadas conforme o perfil do usuário (administrativo, legislativo, TI, etc.).
- Permitir que o usuário autenticado possa ser rastreado individualmente em termos de atividades de rede, permitindo saber quem acessou qual recurso e em que momento.
- Manter registros detalhados das ações de cada usuário, permitindo auditorias e investigações em caso de incidentes de segurança.
- Permitir que o firewall aplique regras de segurança que variam conforme o tipo de usuário (por exemplo, bloqueando certos sites para usuários não administrativos, mas permitindo acessos mais amplos para o TI).
- Integrado com políticas baseadas em identidade, assegurar que somente dispositivos e usuários autorizados possam se conectar à rede.

- Permitir a identificação e classificação do tráfego de rede em diferentes categorias, como tráfego de voz (VoIP), vídeo, dados ou aplicações críticas, assegurando que o tráfego mais importante receba prioridade.
- Possibilitar a limitação da largura de banda para usuários ou aplicações não essenciais, garantindo que o tráfego de alta prioridade, como sistemas internos e comunicação oficial, não seja afetado por atividades menos críticas.
- Permitir a aplicação de regras personalizadas para permitir, bloquear ou limitar o tráfego baseado em endereços IP, portas, protocolo ou usuário.
- Permitir configurar políticas de QoS que priorizam aplicativos essenciais, como sistemas de gestão legislativa ou videoconferências, reduzindo latência e assegurando a entrega contínua de serviços.
- Impedir que tráfego não prioritário, como download de arquivos P2P ou streaming de vídeos, consuma uma quantidade excessiva de largura de banda, afetando a produtividade e a segurança.
- Permitir ajustar o comportamento do tráfego, determinando a largura de banda disponível para diferentes tipos de comunicação, para garantir que o desempenho da rede atenda aos requisitos operacionais da Câmara Municipal.

6.1.2.3. Funções de Segurança:

- Oferecer inspeção detalhada do tráfego na rede, permitindo controlar o que entra e sai, e aplicando políticas de segurança para diferentes tipos de tráfego e usuários.
- Oferecer filtragem de aplicações através de monitoramento e controle sobre quais aplicativos estão sendo utilizados pelos usuários (como redes sociais, ferramentas de produtividade, streaming etc.), garantindo que apenas aplicações autorizadas possam acessar a rede.
- Oferecer monitoramento ativo de todo o tráfego da rede, detectando e bloqueando ataques de intrusões que tentam explorar vulnerabilidades conhecidas em sistemas e aplicativos.
- Oferecer a utilização de um banco de dados constantemente atualizado de assinaturas de ataques, permitindo a identificação de ameaças novas e já conhecidas.

- Oferecer recurso de Analise e inspecionamento do tráfego criptografado para garantir que malwares escondidos em conexões seguras (como HTTPS) não entrem na rede sem serem detectados.
- Oferecer recurso de análise de ameaças em tempo real para identificar e bloquear malwares avançados, ataques de dia zero (zero-day attacks) e ameaças persistentes que tentam passar despercebidas.
- Oferecer recurso de integração com a nuvem para envio de arquivos suspeitos a sandboxing, onde são executados em ambiente seguro para análise de comportamento.
- Permitir o bloqueio de acesso a sites maliciosos, inseguros ou inapropriados, conforme categorias definidas, como pornografia, jogos de azar, malware, phishing e redes sociais.
- Permitir a proteção contra phishing identificando e bloqueando sites fraudulentos que tentam roubar dados de usuários.
- Permitir a configuração de políticas de segurança baseadas em grupos de usuários ou funções específicas (como gerência, TI, administrativo), garantindo que diferentes usuários tenham diferentes níveis de acesso e proteção.
- Permitir a definição e aplicação de políticas de controle de tráfego para garantir que a largura de banda seja alocada de maneira eficiente, priorizando aplicações críticas e limitando o uso de recursos em aplicações não essenciais.
- Permitir a criação de zonas de segurança separadas (VLANs) dentro da rede, onde diferentes departamentos ou tipos de dispositivos (como servidores e estações de trabalho) possam ser isolados, impedindo que ataques internos se espalhem.
- Permitir o monitoramento continuo do tráfego da rede em busca de assinaturas de ameaças conhecidas, como exploits, malwares, ou tentativas de escaneamento de vulnerabilidades.
- examinar pacotes de dados em tempo real e identifica comportamentos anômalos que podem indicar um ataque em andamento, interrompendo imediatamente o tráfego malicioso.

- Bloquear tentativas de exploração de vulnerabilidades conhecidas em sistemas e aplicações, protegendo servidores e estações de trabalho que possam ter falhas não corrigidas (sem patches).
- Integração com bancos de dados globais para garantir que as assinaturas de ameaças sejam atualizadas constantemente.
- Utilização de técnicas avançadas de inspeção de comportamento para bloquear ataques de dia zero (zero-day), que são aqueles para os quais ainda não existe correção ou assinatura no momento da detecção.
- Gerar relatórios detalhados de ataques prevenidos, ajudando a identificar padrões e tendências de tentativas de invasão, fornecendo à equipe de TI insights valiosos para fortalecer a segurança.
- Monitoramento de tentativas de intrusão internas e externas, garantindo uma visão completa da atividade na rede.

6.1.2.4. Garantia e Suporte Técnico para o Appliance Firewall de Próxima Geração (NGFW)

6.1.2.4.1. Garantia

6.1.2.4.1.1. Período de Garantia: O appliance de firewall deverá contar com garantia mínima de 12 meses a partir da data de instalação e ativação do equipamento, sem custos adicionais ao contratante.

6.1.2.4.1.2. Cobertura da Garantia: A garantia deverá cobrir falhas de hardware, defeitos de fabricação, substituição de componentes defeituosos e atualizações de firmware necessárias para manter o firewall em funcionamento otimizado.

6.1.2.4.1.3. Suporte para Atualizações: Durante o período de garantia, todas as atualizações de software e firmware lançadas pelo fabricante deverão ser fornecidas, incluindo patches de segurança, melhorias de desempenho e novas funcionalidades.

6.1.2.4.1.4. Troca de Equipamento Defeituoso: Caso ocorra qualquer falha irreparável no equipamento, o fornecedor deverá garantir a substituição imediata do firewall por um equipamento equivalente ou superior, no prazo máximo de 1 dia útil, com todas as despesas de envio e configuração cobertas.

6.1.2.4.2. Suporte Técnico

6.1.2.4.2.1. Atendimento 24x7: O fornecedor deverá oferecer suporte técnico especializado 24 horas por dia, 7 dias por semana (24x7) para tratar de incidentes críticos, falhas no sistema e problemas de configuração, garantindo a continuidade da operação do ambiente protegido.

6.1.2.4.2.2. Suporte Multicanal: O suporte técnico deverá ser acessível por telefone, e-mail, chat e via um portal web, oferecendo múltiplas formas de contato para atendimento ágil e eficiente.

6.1.2.4.2.3. Tempo de Resposta e Solução: Chamados de suporte técnico relacionados a falhas de segurança ou indisponibilidade do serviço deverão ter tempo de resposta de até 1 hora para incidentes críticos e solução em até 4 horas.

6.1.3. Software Antivírus com XDR (Extended Detection and Response)

6.1.3.1. Especificações Técnicas Mínimas

- Deve ser compatível com os principais sistemas operacionais utilizados pela Câmara Municipal, como Windows e Linux (para desktops e servidores).
- Suporte a ambientes de 32 e 64 bits.
- Capacidade de monitoramento em tempo real de arquivos, downloads, processos e tráfego de rede.
- Análise unificada e correlação de dados de endpoints, servidores, redes e serviços de nuvem para detecção avançada de ameaças.
- O software deve ser atualizado automaticamente, tanto em termos de assinaturas de vírus quanto de atualizações de segurança e funcionalidade.
- Impacto mínimo no desempenho do sistema, evitando o uso excessivo de CPU e memória durante verificações e proteção em tempo real.
- O software deve ser capaz de isolar endpoints comprometidos para impedir que as ameaças se espalhem pela rede.
- Utilização de inteligência artificial (IA) para detecção proativa de ameaças, análise de comportamentos suspeitos e resposta automática a incidentes.
- Suporte para múltiplos dispositivos e servidores, com gerenciamento centralizado de servidores e desktops.

6.1.3.2. Funcionalidades Gerais

- Monitorar o sistema continuamente, detectando e bloqueando ameaças, como vírus, malwares, ransomwares, spywares e trojans, antes que possam infectar o sistema.
- Monitorar o comportamento de processos e aplicativos para detectar atividades suspeitas, mesmo que os arquivos maliciosos não estejam nas bases de dados conhecidas de assinaturas.
- Capacidade de detectar ameaças ainda desconhecidas ou variantes de malwares existentes utilizando algoritmos de inteligência artificial (IA) e machine learning.
- Quando uma ameaça é detectada, o sistema deve isolar o dispositivo, interromper processos maliciosos e realizar ações corretivas automaticamente.
- O software deve permitir configurar verificações completas ou personalizadas, verificando discos, pastas e arquivos específicos com base nas políticas da organização.
- O software deve ter a capacidade de bloquear ou restringir o uso de dispositivos removíveis, como pen drives e discos externos, evitando a introdução de malwares por esses meios.
- Arquivos suspeitos devem ser enviados para um ambiente de sandboxing, onde são executados de forma isolada para análise detalhada de ameaças.

6.1.3.3. Funcionalidades de Gerenciamento e Relatório

- Oferecer plataforma centralizada, baseada em nuvem, que permita monitorar e gerenciar todos os endpoints e servidores protegidos.
- Permitir o acesso a relatórios diários, semanais ou sob demanda sobre a detecção de ameaças, tentativas de exploração de vulnerabilidades e status de conformidade dos sistemas.
- Oferecer registros completos dos eventos de segurança, incluindo detecção, bloqueio e resposta a incidentes de segurança.
- Oferecer painéis de controle com gráficos e visualizações interativas que destacam o status de proteção, ameaças recentes e atividades anômalas detectadas.
- Capacidade de bloquear servidores comprometidos para evitar o acesso e a propagação de ameaças.
- Permitir o monitoramento de alterações em arquivos críticos do sistema, garantindo que quaisquer modificações não autorizadas sejam detectadas imediatamente.

- Identificar vulnerabilidades em softwares e sistemas operacionais, com recomendações de correções ou patches.

6.1.3.4. Funcionalidades de Segurança

- Detecção Multicamadas XDR correlacionando dados de múltiplas fontes (endpoints, redes, servidores, nuvem) para identificar e responder a ameaças avançadas com maior precisão e velocidade.
- Utilizar a análise de dados comportamentais e IA para identificar ameaças que podem passar despercebidas por soluções de segurança convencionais.
- Resposta Coordenada a incidentes e automatizada, isolando endpoints comprometidos, interrompendo processos maliciosos e corrigindo vulnerabilidades em tempo real.
- Visualização e Proteção da Nuvem permitindo visualizar todo o ambiente de nuvem da organização e aplicar políticas de segurança para proteger dados e infraestrutura na nuvem.
- Identificar possíveis configurações incorretas e vulnerabilidades na infraestrutura de nuvem, garantindo que os recursos da nuvem estejam adequadamente protegidos.
- Detectar atividades maliciosas associadas a ransomware interrompendo imediatamente o processo de criptografia, além de oferecer restauração automática dos arquivos afetados.
- Em caso de detecção de ransomware, o software deve permitir a restauração dos arquivos criptografados a partir de backups seguros.
- Detecção Comportamental através de monitoramento constante de atividades anômalas no sistema, como alterações inesperadas em arquivos ou processos que desviam do comportamento normal, bloqueando ações suspeitas em tempo real.
- Gerenciamento de Permissões sobre quais usuários e dispositivos podem acessar arquivos e sistemas críticos, garantindo que apenas pessoal autorizado tenha acesso.
- Tecnologia de Prevenção de Exploits **p**rotegendo contra vulnerabilidades conhecidas e desconhecidas, bloqueando tentativas de explorar falhas de segurança em aplicativos e sistemas operacionais.
- **Monitoramento de Processos** verificando e bloqueando processos suspeitos que tentam explorar vulnerabilidades para ganhar acesso não autorizado ao sistema.

6.1.4. Suporte Técnico:

6.1.4.1. Garantia

6.1.4.1.1. Período de Garantia: A solução de software antivírus com recursos XDR deverá contar com garantia mínima de 12 meses a partir da data de instalação e ativação do produto, sem custos adicionais ao contratante.

6.1.4.1.2. Cobertura da Garantia: A garantia deverá cobrir todas as atualizações e melhorias do software durante o período contratado, incluindo patches de segurança, correções de vulnerabilidades e atualizações de versão.

6.1.4.1.3. Suporte para Atualizações: O suporte técnico deverá incluir a assistência na aplicação de atualizações e melhorias críticas, garantindo que o software esteja sempre atualizado e otimizado contra novas ameaças.

6.1.4.2. Suporte Técnico

6.1.4.2.1. Atendimento 24x7: O fornecedor deverá disponibilizar suporte técnico contínuo (24 horas por dia, 7 dias por semana), com equipe capacitada para resolver incidentes de segurança, problemas técnicos e prestar auxílio na configuração e manutenção do software**.**

6.1.4.2.2. Suporte Multicanal: Suporte deverá ser fornecido através de diferentes canais, incluindo telefone, e-mail e chat online, além de um portal de autoatendimento com base de conhecimento e FAQs**.**

6.1.4.2.3. Escalonamento de Problemas: Em caso de problemas complexos ou de difícil solução, o fornecedor deverá garantir escalonamento para engenheiros especializados e, se necessário, equipes de desenvolvimento do software para garantir a solução rápida e eficaz.

7. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

7.1. Especialização Técnica Distinta

7.1.1. O parcelamento permite que a contratação seja feita com empresas especializadas em diferentes segmentos:

7.1.2. **Appliances de firewall de próxima geração (NGFW)**: Fabricantes e fornecedores especializados em hardware de segurança podem oferecer soluções com suporte técnico mais avançado e conhecimento específico sobre a configuração e implementação de firewalls.

7.1.3. **Software antivírus com XDR**: Fornecedores de software antivírus que atuam exclusivamente nessa área podem oferecer um nível de suporte mais especializado, além de atualizações contínuas e um foco em inovação tecnológica para detecção e resposta a ameaças.

7.1.4. Essa segmentação maximiza a qualidade do serviço, garantindo que cada parte da solução de segurança seja tratada por especialistas.

7.2. Vantagem Competitiva e Melhores Preços

7.2.1. O parcelamento permite a participação de um maior número de empresas, tanto na licitação para o firewall NGFW quanto para o software antivírus com XDR, aumentando a competitividade. Esse aumento de concorrência pode resultar em:

7.2.1.1. **Preços mais competitivos**: Mais empresas podem participar de cada lote específico, o que pode reduzir os custos ao proporcionar melhores ofertas.

7.2.1.2. **Negociações específicas**: O parcelamento facilita negociações independentes com fornecedores, permitindo que a Câmara obtenha condições financeiras mais vantajosas para cada parte da solução de segurança.

7.3. Redução de Riscos e Menor Dependência de um Único Fornecedor

7.3.1. O parcelamento diminui os riscos associados à contratação de um único fornecedor para toda a solução. Entre os principais benefícios estão:

7.3.1.1. Distribuição de riscos: Contratar diferentes fornecedores reduz a dependência de um único prestador de serviços, mitigando possíveis falhas ou deficiências em um dos contratos.

7.3.1.2. Possibilidade de substituições: Caso um dos fornecedores não atenda às expectativas, o contrato pode ser ajustado ou substituído sem comprometer toda a solução de segurança cibernética da Câmara.

7.4. Conclusão

7.4.1. O parcelamento da contratação de appliances de firewall NGFW e licenças de software antivírus XDR para desktops e servidores oferece vantagens em termos de especialização técnica, competitividade de preços, flexibilidade de implementação e gestão de riscos. Essa estratégia também permite maior controle sobre o orçamento e possibilita a adaptação a novas tecnologias, garantindo que a Câmara Municipal de Itanhaém mantenha suas soluções de segurança cibernética sempre atualizadas e eficazes.

8. DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS EM TERMOS DE ECONOMICIDADE E DE MELHOR APROVEITAMENTO DOS RECURSOS HUMANOS, MATERIAIS OU FINANCEIROS DISPONÍVEIS

8.1. A contratação dos appliances de firewall NGFW e das licenças de software antivírus com XDR para a Câmara Municipal visa alcançar melhorias significativas em segurança cibernética, eficiência operacional e gestão financeira. Abaixo estão detalhados os principais benefícios em termos de economicidade e de melhor aproveitamento dos recursos humanos, materiais e financeiros.

8.1.1. Economicidade

8.1.1.1. Redução de Custos por Competitividade

8.1.1.1.1. Ao separar a aquisição dos appliances de firewall NGFW e das licenças de antivírus XDR, a Câmara Municipal de Itanhaém pode obter condições mais favoráveis através de concorrência direta nos dois mercados:

8.1.1.1.1.1. Maior número de fornecedores especializados: A separação abre espaço para que empresas especializadas em cada tecnologia ofereçam propostas mais competitivas, possibilitando uma redução de preços ao ampliar o leque de fornecedores participantes.

8.1.2. Melhor Aproveitamento dos Recursos Humanos

8.1.2.1. Acompanhamento gradual de desempenho: Cada solução pode ser implementada e gerida de maneira independente, permitindo um acompanhamento mais preciso dos resultados e ajustes necessários.

8.1.3. Alocação Gradual de Recursos Humanos

8.1.3.1. Menor impacto operacional: A implantação faseada reduz a necessidade de sobrecarga imediata sobre a equipe de TI, uma vez que o foco será direcionado para uma solução por vez.

8.1.3.2. Ajuste no uso da equipe de TI: Ao trabalhar com duas frentes separadas, a equipe pode se organizar para otimizar o tempo de gestão de cada um dos sistemas sem afetar a operação contínua de outros setores.

8.1.4. Melhor Aproveitamento dos Recursos Materiais

8.1.4.1. Aprimoramento gradual da segurança: A contratação do firewall NGFW pode ocorrer em um primeiro momento para assegurar a proteção de perímetro, enquanto as licenças de antivírus XDR podem ser adquiridas conforme a necessidade de proteção endpoint cresce, possibilitando a evolução modular da infraestrutura.

8.1.4.2. Utilização mais eficiente de recursos existentes: Separar as aquisições permite que os equipamentos e softwares antigos sejam substituídos de forma ordenada, garantindo que não haja ociosidade de recursos.

8.1.5. Melhor Aproveitamento dos Recursos Financeiros

8.1.5.1. Ao contratar cada solução de maneira independente, é possível ajustar o suporte técnico conforme as características de cada produto:

8.1.5.1.1. Suporte específico para cada solução: A separação permite que contratos de suporte técnico sejam negociados de acordo com a complexidade e criticidade de cada solução, evitando custos elevados com pacotes abrangentes que muitas vezes cobrem mais do que o necessário.

8.1.5.1.2. Acompanhamento financeiro mais preciso: Com contratos separados, a Câmara pode monitorar os custos de suporte e manutenção de forma individualizada, promovendo ajustes conforme o uso de cada sistema.

8.1.5.1.3. Renovação independente: A separação permite renovar ou ajustar contratos conforme o ciclo de vida de cada solução, sem comprometer o outro sistema. Isso garante que a Câmara pague apenas pelo que realmente precisa e no momento certo.

9. PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO PREVIAMENTE À CELEBRAÇÃO DO CONTRATO

9.1. A Administração deverá definir, previamente à assinatura do contrato, os servidores responsáveis pela fiscalização e gestão contratual.

10. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

10.2. Não há correlação com outras contratações.

11. DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS MITIGADORAS

11.1. Não há efeitos de impactos ambientais.

12. POSICIONAMENTO CONCLUSIVO SOBRE A ADEQUAÇÃO DA CONTRATAÇÃO PARA O ATENDIMENTO DA NECESSIDADE A QUE SE DESTINA

12.1. A contratação requerida alinha-se às finalidades da Câmara Municipal e mostra-se viável sob às óticas ambiental, econômico e estratégica, conforme demonstrado neste estudo;

12.2. Os requisitos relevantes para a contratação foram devidamente levantados e analisados;

12.3. As quantidades são condizentes com a demanda prevista;

12.4. Existe no mercado a solução proposta que garante a concorrência;

12.5. A estimativa preliminar de preços foi realizada e documentada;

12.6. Foram indicados os resultados pretendidos com a contratação.

Itanhaém, 06 de setembro de 2024

ALLAN BELLUCCI

DIRETOR DE TECNOLOGIA DA INFORMAÇÃO