Governo do Estado de São Paulo
Companhia Paulista de Trens Metropolitanos
Depto De Contratacoes E Compras

TERMO ADITIVO

CONTRATO Nº 072222305100-02

PROCESSO Nº 0722223051 - 386.00000264/2023-71
CONTRATO PRODESP NUMERO: PD022474

TERMO DE ADITAMENTO Nº 02 AO CONTRATO Nº 072222305100 CELEBRADO ENTRE A COMPANHIA PAULISTA DE TRENS METROPOLITANOS – CPTM E A COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO - PRODESP.

Pelo presente instrumento, elaborado para um único efeito, as partes abaixo assinadas, de um lado a **COMPANHIA PAULISTA DE TRENS METROPOLITANOS - CPTM**, CNPJ nº 71.832.679/0001-23, com sede em São Paulo/SP, na Rua Boa Vista, 185, Centro, doravante denominada simplesmente **CPTM**, por seus representantes legais, e, de outro lado, a **COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO - PRODESP**, CNPJ nº 62.577.929/0001-35, com sede em Taboão da Serra/SP, na Rua Águeda Gonçalves nº 240 – Jardim Pedro Gonçalves e filiais CNPJ nº 62.577.929/0114-12 situada em São Paulo/SP, na Rua da Mooca nº 1921 – Mooca e CNPJ nº 62.577.929/0043-94 situada em Osasco/SP, na Avenida Hilário Pereira de Souza nº 664 – Centro, doravante denominada simplesmente **CONTRATADA**, por seu representante legal, concordam em

aditar o contrato firmado para a **PRESTAÇÃO DE SERVIÇOS ESPECIALIZADOS EM TI – TECNOLOGIA DA INFORMAÇÃO, QUE SE CONSTITUEM DE UMA SOLUÇÃO GLOBAL AO AMBIENTE DE TI, A SABER: ATENDIMENTO E SUPORTE AO USUÁRIO DE TI E SERVIÇOS NO AMBIENTE DE TI**, ajustando e convencionando as obrigações e compromissos recíprocos, na forma da Lei Federal n° 13.303, de 30 de junho de 2016, do Regulamento de Licitações, Contratos e Demais Ajustes da Companhia Paulista de Trens Metropolitanos - CPTM - Vigente a partir de 17/05/2022, da Lei Complementar n° 123, de 14/12/2006, as disposições do Capítulo II-B do Título XI da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), das normas internas específicas da CPTM, do Código de Conduta e Integridade da CPTM, do Código de Conduta e Integridade de Fornecedores, Prestadores de Serviços e Parceiros da CPTM, da Lei Federal nº 13.709, de 14 de agosto de 2018, com suas alterações subsequentes, bem como toda a legislação aplicável sobre privacidade e proteção de dados, inclusive, normas setoriais ou gerais sobre o tema, no âmbito da execução do objeto deste Contrato, pelas condições constantes das demais normas regulamentares aplicáveis à espécie, nas condições estabelecidas nas seguintes cláusulas:

1 OBJETO

1.1 O presente Termo de Aditamento tem por finalidade a readequação da planilha de quantidades e preços, conforme Planilha de Quantidades e Preços – Anexo 1, Termo de Referência - Anexo 2 e Especificação de Serviço e Preço ESP E0220920-T01 – Anexo 3, todos deste instrumento.

2 VALOR

2.1 Em razão do presente aditamento, o valor do contrato passará a ser de R$ 52.592.478,35 (cinquenta e dois milhões, quinhentos e noventa e dois mil, quatrocentos e setenta e oito reais e trinta e cinco centavos), data base novembro /2022.

3 RATIFICAÇÃO

3.1 Ficam ratificadas as demais Cláusulas do Contrato nº 072222305100 e do Termo de Aditamento nº 01 que não foram objeto de alteração pelo presente instrumento.

E por estarem justas e contratadas firmam o presente, na presença das testemunhas.

Pela **COMPANHIA PAULISTA DE TRENS METROPOLITANOS - CPTM**:

ANA CAROLINE DE FARIA EDUARDO BORGES
Diretora Administrativa e Financeira
ana.borges@cptm.sp.gov.br
e-mail pessoal: N/I
CPF nº 003.938.371-73
RG nº 4.296.749

PEDRO TEGON MORO
Diretor Presidente
pedro.moro@cptm.sp.gov.br
e-mail pessoal: N/I
CPF nº 144.051.718-58
RG nº 21.448.592-4

JOSÉ LUIZ BARCI NEVES
Gerente de Tecnologia da Informação
jose.barci@cptm.sp.gov.br
e-mail pessoal: N/I
CPF nº 853.555.507-20
RG nº 39.326.561-4

Pela **COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO - PRODESP**:

FERNANDO HIDEYO YOKEMURA
Diretor de Operações
yokemura@sp.gov.br
e -mail pessoal: N/I
CPF nº 517.724.930-15
RG nº 20.349.698-21

RAFAEL ALMEIDA FERNANDEZ SOTO
Diretor de Desenvolvimento e Sistemas
rafael.soto@sp.gov.br
e-mail pessoal: N/I
CPF nº 010.570.755-40
RG nº 09.090.434-69

TESTEMUNHAS:

FERNANDO AUGUSTO KOGA
Assessor Executivo

MARIANA MIDORI KAWANO
Analista de Processos de Contratação

	Documento assinado eletronicamente por **Rafael Almeida Fernandez Soto**, **Diretor**, em 10/05/2024, às 17:44, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.
	Documento assinado eletronicamente por **Fernando Hideyo Yokemura**, **Diretor**, em 10/05/2024, às 18:00, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.
	Documento assinado eletronicamente por **Mariana Midori Kawano**, **ANL De Processos De Contratacao**, em 10/05/2024, às 18:01, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.
	Documento assinado eletronicamente por **Fernando Augusto Koga**, **Assessor Executivo**, em 10/05/2024, às 18:01, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.
	Documento assinado eletronicamente por **Jose Luiz Barci Neves**, **Gerente**, em 10/05/2024, às 18:05, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.
	Documento assinado eletronicamente por **Ana Caroline de Faria Eduardo Borges**, **Diretor**, em 10/05/2024, às 18:23, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.
	Documento assinado eletronicamente por **Pedro Tegon Moro**, **Diretor Presidente**, em 10/05/2024, às 19:34, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

 A autenticidade deste documento pode ser conferida no site https://sei.sp.gov.br/sei/controlador_externo.php?

acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0027635839** e o código CRC **A64F7835**.

ANEXO 1

TERMO DE ADITAMENTO Nº 02 AO CONTRATO Nº 072222305100

PLANILHA DE QUANTIDADES E PREÇOS PROPOSTOS

Prodesp

Governo do Estado de São Paulo
Companhia de Processamento de Dados do Estado de São Paulo
Coordenadoria de Novos Negócios

PLANILHA DE ORÇAMENTO ESPECIFICAÇÃO DE SERVIÇOS E PREÇOS

Prodesp .GOV.BR

ANEXO I
PLANILHA DE ORÇAMENTO
ESPECIFICAÇÃO DE SERVIÇOS E PREÇOS E0220920-T01
CONTRATO PD022474-T02 (ADITAMENTO)
COMPANHIA PAULISTA DE TRENS METROPOLITANOS - CPTM

ITEM	DESCRIÇÃO DOS SERVIÇOS	PARCELA ÚNICA	VALOR MENSAL	TOTAL PREVISTO	ADITAMENTO
5.1	ATENDIMENTO E SUPORTE AO USUÁRIO DE TI	R$ -	R$ 133.727,04	R$ 4.011.811,20	R$ -
5.2	SUPORTE LOCAL	R$ -	R$ 300.901,44	R$ 9.027.043,20	R$ -
5.3	GERENCIAMENTO DE SEGURANÇA	R$ -	R$ 108.853,74	R$ 3.265.612,20	R$ -
5.4	GESTÃO E OPERAÇÃO DO AMBIENTE DE TI	R$ 164.568,40	R$ 42.460,72	R$ 1.438.390,00	R$ -
5.5	GESTÃO DE SERVIDORES E ARMAZENAMENTO, E APOIO A BANCO DE DADOS	R$ -	R$ 937.392,62	R$ 28.121.778,60	R$ -
5.6	Implementação de novas camadas de Proteção ao Trend Micro Apex One (ADITAMENTO)	R$ 2.192.893,74	R$ 323.924,96	R$ 6.727.843,15	R$ 6.727.843,15
TOTAL		R$ 2.357.462,14	R$ 1.847.260,52	R$ 52.592.478,35	R$ 6.727.843,15

TOTAL (TERMO 0)	R$ 164.568,40	R$ 1.523.335,56	R$ 45.864.635,20

TOTAL ADITAMENTO	R$ 2.192.893,74	R$ 323.924,96	R$ 6.727.843,15	14,6700%

Documento assinado eletronicamente por **Paul Michel de Souza Haro**, **Assessor**, em 09/05/2024, às 15:44, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Kelly Cristine Da Silva Ferreira**, **Coordenador**, em 09/05/2024, às 16:50, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

A autenticidade deste documento pode ser conferida no site https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0026981780** e o código CRC **6B71B151**.

ANEXO 2

TERMO DE ADITAMENTO Nº 02 AO CONTRATO Nº 072222305100

TERMO DE REFERÊNCIA

TERMO DE REFERÊNCIA

OBJETO

AMPLIAÇÃO DA SOLUÇÃO EXISTENTE DE SEGURANÇA AVANÇADA PARA O AMBIENTE COMPUTACIONAL DA CPTM

TR. DFIM.001/2024 **janeiro/2024**

Sumário

1. OBJETO **4**

2. CARACTERÍSTICAS GERAIS **4**

3. ESPECIFICAÇÃO TÉCNICA **5**

4. IMPLANTAÇÃO **37**

5. RELATÓRIOS **40**

6. SUPORTE TÉCNICO DA SOLUÇÃO **42**

7. ACORDO DE NÍVEL DE SERVIÇO **43**

8. ATUALIZAÇÕES E MANUTENÇÕES **45**

9. PRAZOS, ENTREGAS E RECEBIMENTOS **48**

10. MEDIÇÃO **49**

11. CONDIÇÕES DE PAGAMENTO **50**

12. EXECUÇÃO DOS SERVIÇOS **51**

13. ANEXO I – PLANILHA DE QUANTIDADES E PREÇOS **52**

1. OBJETO

1.1. AMPLIAÇÃO DA SOLUÇÃO EXISTENTE DE SEGURANÇA AVANÇADA PARA O AMBIENTE COMPUTACIONAL DA CPTM.

2. CARACTERÍSTICAS GERAIS

2.1. A solução descrita neste documento, com base nas características técnicas especificadas, busca elevar o nível de segurança existente ao patamar desejado pela gestão da empresa, através da implementação de uma plataforma de cibersegurança composta de tecnologias de hardware e software, visando ampliar as camadas de segurança, bem como fornecer autonomia para que sua equipe técnica, responsável pela vertical de segurança, atue de forma a impedir e paralisar imediatamente e de forma eficaz, quaisquer ataques ou tentativas de ataques cibernéticos contra a CPTM.

2.2. As soluções a serem ofertadas deverão minimamente atender na integra a todas as especificações técnicas contidas neste documento, não se limitando a estas.

2.3. A solução deverá se adequar às necessidades da CPTM, com as seguintes características:

2.3.1. Inspeção de tráfego de rede (Troughput) diário

2.3.2. Sensor de Detecção e Resposta para Servidores de Rede

2.3.3. Console de gerenciamento unificada da plataforma de detecção e resposta estendida

2.4. A plataforma de segurança unificada deverá possuir console única de gerenciamento, para extensão de visibilidade do ambiente, fornecendo quantificação de risco, baseado na identificação e mapeamento da superfície de ataque.

2.5. Todo as licenças de uso de software ou hardware necessárias para atender as especificações técnicas deste documento deverão estar disponíveis para uso imediato.

2.6. PLATAFORMA DE CIBERSEGURANÇA

2.6.1. Plataforma de segurança unificada para extensão de visibilidade do ambiente, quantificação de risco, baseado na identificação e mapeamento da superfície de ataque.

2.6.2. Para atender a integridade da solução e facilitar a gestão do ambiente, todos os componentes da solução deverão ser do mesmo fabricante.

2.7. COMPOSIÇÃO DA SOLUÇÃO

ITEM	DECRIÇÃO DO ITEM
1	Solução de inspeção de rede contra ameaças avançadas com detecção e resposta.
2	Solução de segurança para servidores e cargas de trabalho híbridas com detecção e resposta.
3	Console de gerenciamento unificada da plataforma com detecção e resposta estendida para extensão de visibilidade do ambiente e ação imediata contra ameaças.
4	Serviço de manutenção e suporte
5	Serviços de implantação e configuração

3. ESPECIFICAÇÃO TÉCNICA

3.1. Solução de inspeção de rede contra ameaças avançadas com detecção e resposta.

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

3.1.2. O sensor avançado de análise de rede deverá ser licenciado a fim de inspecionar o Throughput total da CONTRATANTE;

3.1.3. Deverá atuar com a inspeção de rede da CONTRATANTE, estendendo visibilidade sob tráfego leste-oeste e norte-sul;

3.1.4. O Sensor deverá ser instalado de modo a detectar ameaças avançadas no ambiente da CONTRATANTE, inspecionando o tráfego de rede, independente de agentes instalados;

3.1.5. O sensor deverá ser instalado a fim de detectar ameaças avançadas no ambiente da CONTRATANTE, inspecionando o tráfego de rede, independente de agentes instalados;

3.1.6. O sensor deverá aplicar técnicas de análise de tráfego avançadas baseadas em aprendizagem de máquina;

3.1.7. O sensor deverá atuar com técnicas de detecção e resposta específicos para modelos de detecção focados em rede, de forma a identificar comportamentos maliciosos;

3.1.8. O sensor deverá permitir que seja implantado em linha com o tráfego de rede e em modo de espelhamento de rede;

3.1.9. Caso seja implementada em linha na rede da CONTRATANTE, o sensor deverá permitir a criação de regras de by-pass para casos de falhas de interface;

3.1.10. Deverá suportar o uso de portas espelhadas de switch (mirror port) para monitorar o tráfego e detectar potenciais riscos à Segurança;

3.1.11. Durante a inspeção do tráfego de rede em tempo real, o sensor deverá ser capaz de identificar anomalias na rede e gerar alertas em casos de tráfego suspeito;

3.1.12. Deverá implementar características de Network Detection and Response baseado em comportamento;

3.1.13. Quando implantada em linha com a rede da CONTRATANTE, o sensor deverá ter a capacidade de analisar tráfego TLS, sem necessidade de licenciamento adicional;

3.1.14. Deverá identificar ameaças direcionadas avançadas e persistentes (APT);

3.1.15. Deverá analisar possíveis fases de um ataque direcionado, identificando tentativas de coletas de informação, movimentação lateral, exfiltração de dados, descoberta de dispositivos e comunicações de comando e controle (C&C);

3.1.16. Deverá identificar e mapear possíveis pontos de entrada na rede que possam ser exploradas por atacantes;

3.1.17. Deverá prover automatizações para bloqueio de ameaças identificadas a partir da inspeção de rede;

3.1.18. O Sensor deverá inspecionar a rede a fim de analisar, no mínimo os protocolos: HTTP, HTTPS, LDAP, FTP, Telnet, WebSocket, SMTP, POP3, DNS, SMB, RDP, Kerberos, IRC, VNC, SQL, MYSQL e ARP.

3.1.19. Deverá permitir análise de arquivos em sandbox, permitindo identificar ataques avançados (APT), Zero Days, códigos de exploração (exploits) embutidos, vulnerabilidades conhecidas e arquivos maliciosos no tráfego de rede, de forma automática e quando aplicável;

3.1.20. Deverá analisar em tempo real o comportamento através de simulação de execução de arquivos provenientes do tráfego de rede incluindo arquivos executáveis (scripts), PDF´s, executáveis, PPTX, DOCX, XLSX, LNK, ELF, CHM, RTF, ODP, DLLs, JAR, ZIP e RAR;

3.1.21. O sensor de inspeção de rede, deverá possuir capacidade de envio de artefatos para analisador virtual dedicado, externo, sendo que este deverá suportar no mínimo os sistemas operacionais Linux, Windows 10, Windows Server, 2008, 2012 R2, 2016 e 2019;

3.1.22. Deverá suportar a criação de sandboxes que repliquem os sistemas operacionais e aplicações da CONTRATANTE, para avaliação do real impacto da ameaça no ambiente;

3.1.23. Deverá possibilitar a predefinição de políticas para determinar quais tipos de arquivos deverão ser enviados para análise;

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

3.1.25. Deverá possuir atualização automática de regras, sendo que estas deverão ser disponibilizadas via internet pelo fabricante da solução durante o período de vigência do contrato de suporte e manutenção;

3.1.26. Deverá ser capaz de identificar movimentos laterais em toda a rede corporativa;

3.1.27. Deverá possuir interface web para busca e investigação local de incidentes;

3.1.28. Capacidade de detectar ameaças web derivadas de vulnerabilidades e downloads de conteúdo malicioso;

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

3.1.30. A solução deverá ser capaz de analisar protocolos mascarados ou tunelados em ICMP, IP, UDP e TCP;

3.1.31. Deverá ser capaz de detectar ameaças desconhecidas, ataques dirigidos e ameaças de dia zero, sendo que este módulo majoritariamente deverá pertencer ao mesmo fabricante;

3.1.32. Deverá permitir o rastreio por malwares utilizando métodos de detecção baseados no tipo de arquivo, múltiplas camadas de empacotamento e arquivos comprimidos;

3.1.33. Deverá suportar o monitoramento de múltiplas interfaces de rede conectadas a diferentes VLANs e Switches;

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

3.1.35. Deverá possibilitar que modelos de detecção a nível de rede sejam customizados de acordo com as necessidades da CONTRATANTE;

3.1.36. Deverá possuir regras que identifiquem comunicações dos seguintes tipos: C&C, Exploits, Executáveis Maliciosos, Comunicação com Sites Maliciosos, backdoors e escaneamentos de porta;

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

3.1.38. Deverá possuir regras que identifiquem comunicações streaming de mídia, peer-to-peer e instant messengers;

3.1.39. Deverá possuir capacidade de geração de relatórios dos seguintes tipos e contendo as seguintes características:

3.1.39.1. Sumário das detecções;

3.1.39.2. Visão Geral dos Incidentes de Segurança;

3.1.39.3. Discriminação dos Tipos de Incidentes;

3.1.39.4. Top Ameaças Analisadas;

3.1.39.5. Top Hosts Infectados;

3.1.39.6. Recomendações de Segurança;

3.1.39.7. Executivos.

3.1.40. Deverá possuir detalhes técnicos dos incidentes detectados;

3.1.41. Deverá possuir estatística do tráfego analisado;

3.1.42. Deverá possuir indicadores de risco do ambiente;

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

3.1.44. Deverá permitir o upgrade e downgrade de versão de firmware;

3.1.45. Deverá ser capaz de detectar tentativas de mascaramento ou evasão de detecção através do uso de portas comuns e tunelamento de protocolo;

3.1.46. Deverá ser capaz de detectar tentativas de escaneamento de rede;

3.1.47. Deverá ser capaz de detectar propagação de malwares na rede;

3.1.48. Deverá ser capaz de detectar tentativas de força bruta em credenciais;

3.1.49. Deverá ser capaz de detectar tentativas de roubo de informação;

3.1.50. Deverá ser capaz de detectar ameaças que se replicam na rede;

3.1.51. Deverá ser capaz de detectar Exploits na rede;

3.1.52. Deverá replicar a comunicação captada por interface gráfica interativa, a fim de facilitar a compreensão dos alertas gerados;

3.1.53. Deverá possuir interface gráfica que apresente em tempo real estatísticas de top ameaças detectadas, top arquivos analisados, top hosts afetados, top URL's maliciosas acessadas etc.;

3.1.54. Deverá apresentar panorama de detecções de comunicações suspeitas e maliciosas baseado em geolocalização, onde são marcadas origens geográficas de ataques e eventos de segurança monitorados pela solução, por meio de dashboard;

3.1.55. Deverá possuir interface gráfica que apresente em tempo real estatísticas de top ameaças detectadas, top arquivos analisados, top hosts afetados, top URL's maliciosas acessadas etc.;

3.1.56. Deverá apresentar panorama de detecções de comunicações suspeitas e maliciosas baseado em geolocalização, onde são marcadas origens geográficas de ataques e eventos de segurança monitorados pela solução, por meio de dashboard;

3.1.57. Deverá permitir busca por informações de destino e origem de comunicações, incluindo: endereço IP, endereço MAC, domínio, protocolo e grupo de rede;

3.1.58. Deverá permitir consultas personalizáveis, usando comandos SQL ou atributos pré-definidos;

3.1.59. Deverá possuir:

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

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

3.1.59.3. Capacidade de gerar relatórios baseados nas investigações.

3.1.60. Deverá permitir exportar sob demanda os logs padrões CSV ou PDF;

3.1.61. Deverá permitir consultas personalizáveis, usando comandos SQL ou atributos pré-definidos;

3.1.62. Deverá ser totalmente integrado com a console de gerência da plataforma do próprio fabricante, com objetivo de correlacionar as detecções do sensor de rede com as demais tecnologias de segurança implantadas nas camadas de endpoint, servidores e gateway seguro;

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

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

3.1.65. O sensor de inspeção de rede deverá ter a capacidade de integrar-se com a plataforma de gerência centralizada, a fim de enviar objetos suspeitos e metadados das detecções locais para correlação com as demais soluções de segurança do ambiente;

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

3.1.66.1. Uso de CPU

3.1.66.2. Uso de Disco;

3.1.66.3. Uso de Memória;

3.1.66.4. Tráfego malicioso analisado;

3.1.66.5. Todo o tráfego analisado.

3.1.67. A solução deverá permitir integração com ferramentas de SIEM;

3.1.68. A solução deverá permitir o envio de logs dos recursos para servidor de logs por meio do protocolo syslog com as seguintes características:

3.1.68.1. Suportar ao menos a integração com dois servidores syslogs;

3.1.68.2. Registrar eventos de sistemas e atualizações.

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

3.1.70. A solução deverá ter capacidade de agregação e correlação de logs de eventos de segurança possibilitando coleta de fontes de monitoração para proporcionar informação e identificação de ameaças digitais conhecidas e desconhecidas em trânsito através de logs de sensor;

3.1.71. Deverá listar os 10 hosts mais críticos do ambiente da CONTRATANTE, de forma a categorizá-los de acordo com a severidade atual baseada em número e criticidade das detecções, segundo:

3.1.71.1. Nível Crítico

3.1.71.2. Nível Alto

3.1.71.3. Nível Médio

3.1.71.4. Nível Baixo

3.1.72. Deverá correlacionar cada host listado a um alerta de investigação, quando aplicável;

3.1.73. As detecções de cada host listado deverão ser apresentadas com detalhes para devida investigação;

3.1.74. Deverá apresentar os logs de rede de maneira evidente e destaca por meio de rótulo e cor, a fim de diferenciar dos demais logs de outros sensores;

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

3.1.75.1. Computadores infectados;

3.1.75.2. Origem de infecções;

3.1.75.3. Estatísticas de ameaças;

3.1.75.4. Riscos potenciais de segurança;

3.1.75.5. Riscos de perda de informações;

3.1.75.6. Risco de sistema comprometido;

3.1.75.7. Risco de disseminação de ameaças;

3.1.75.8. Infecções de malware;

3.1.75.9. Eventos suspeitos.

3.1.76. Deverá permitir a configuração de alarmes personalizados, com base em investigações;

3.1.77. Deverá trabalhar com geolocalização para identificar a origem geográfica de um ataque;

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

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

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

3.1.80.1. Requisições GET

3.1.80.2. Requisições POST

3.1.80.3. Requisições MOVED

3.1.80.4. Requisições NOT FOUND

3.1.81. A partir de um alerta do sensor de rede, deverá ser possível o bloqueio dos IPs e URLs envolvidos no contexto da detecção;

3.1.82. Deverá mapear os métodos de requisições detectados ao longo de uma comunicação inspecionada, listando ao menos:

3.1.83. A partir dos alertas gerados, deverá correlacionar as máquinas, IPs e Hashs envolvidos, apontando possíveis indicadores de comprometimento (IOCs) ao ambiente da CONTRATANTE;

3.1.84. Os relatórios e logs deverão ser exportados nos formatos PDF, TXT ou CSV;

3.1.85. O sensor deverá, por meio da integração com a plataforma de detecção e resposta, compartilhar os IOCs com outros sensores do fabricante e ferramentas de terceiros, sendo estas, no mínimo, Fortinet, Palo Alto ou Checkpoint.

3.2. Solução de segurança para servidores e cargas de trabalho híbridas com detecção e resposta

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

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

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

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

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

3.2.6. A solução deverá permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob demanda, ou por tarefa agendada com o envio automático do relatório por e-mail;

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

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

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

3.2.10. Em caso de solução em nuvem, o ambiente do fabricante deverá fornecer alta disponibilidade;

3.2.11. A solução de segurança deverá possuir a capacidade de identificar ataques em estruturas de container.

3.2.12. Deverá ser possível customizar os privilégios de administração da solução:

3.2.12.1. Acesso total;

3.2.12.2. Acesso somente leitura.

3.2.13. Deverá ser possível assignar políticas de segurança em máquinas específicas, grupos estáticos e dinâmicos;

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

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

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

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

3.2.17.1. Windows Server 2008 e 2008 R2;

3.2.17.2. Windows Server 2012 e 2012 R2;

3.2.17.3. Windows Server 2016;

3.2.17.4. Windows Server 2019;

3.2.17.5. Windows Server 2022;

3.2.17.6. Red Hat Enterprise 5, 6, 7 e 8;

3.2.17.7. Oracle Linux 5, 6, 7 e 8;

3.2.17.8. SUSE Linux Enterprise Server 10, 11, 12 e 15;

3.2.17.9. Ubuntu 10, 12, 14, 16, 18 e 20;

3.2.17.10. Debian 6, 7, 8, 9 e 10;

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

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

3.2.20. Os agentes para plataforma Linux deverão ser instalados por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a

proporcionar maior segurança ao ambiente, ou de forma automatizada através de bash script;

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

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

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

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

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

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

3.2.27. A solução deverá mostrar quais máquinas estão usando determinada política;

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

3.2.29. Esses rastreamentos deverão ocorrer de forma periódica a ser definida pelo administrador;

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

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

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

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

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

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

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

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

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

3.2.39. Deverá permitir enviar os relatórios para uma lista de contatos independente de login no console de administração;

3.2.40. As atualizações de assinaturas deverão ocorrer de forma agendada e automática possibilitando envios de hora em hora ou em intervalos definidos;

3.2.41. Após a atualização deverá ser informado o que foi modificado ou adicionado;

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

3.2.43. A console de gerenciamento deverá apresentar a capacidade de gerar roll back de suas atualizações de regras;

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

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

3.2.46. No gerenciamento de licenças, deverá ser informada quantidade contratada e quantidade em utilização de clientes;

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

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

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

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

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

3.2.52. O fabricante da solução deverá manter programa de pesquisa em vulnerabilidades há, pelo menos, 5 anos;

3.2.53. A solução deverá possuir API documentada para integração na esteira de automação;

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

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

3.2.56. A solução deverá permitir desabilitar os módulos individualmente;

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

3.2.58. A console deverá possibilitar a integração com o Microsoft Active Directory, listando as máquinas e grupos existentes na estrutura;

3.2.59. Em caso de a solução ser ofertada em nuvem, deverá ser certificada através de documentação emitida pelos órgãos certificadores para ISO 27001, ISO 27014, ISO 27017 e SOC 2;

3.2.60. Os ambientes em nuvem providos pelo fabricante deverão passar por testes de penetração, com relatórios e metodologias recomendadas como melhores práticas, de forma recorrente para garantir a segurança da solução provida;

3.2.61. Deverá possuir funcionalidade de Antimalware;

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

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

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

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

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

3.2.67. Em servidores Windows, deverá identificar e bloquear ameaças através de métodos de Machine Learning, movendo para quarentena os arquivos identificados;

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

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

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

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

3.2.72. Para servidores Windows, a solução deverá permitir que o escaneamento agendado ocorra, ainda que o agente esteja offline no console de gerenciamento;

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

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

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

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

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

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

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

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

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

3.2.82. A solução ofertada deverá prover as seguintes proteções contra URLs Maliciosas:

3.2.82.1. Deverá permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação;

3.2.82.2. Fornecer lista de URLs atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;

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

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

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

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

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

3.2.82.8. A proteção deverá possibilitar proteção através da instalação de agente de segurança do fabricante da solução de segurança.

3.2.83. Deverá possuir funcionalidade de Firewall de host;

3.2.84. Operar como firewall de host, através da instalação de agentes nos servidores protegidos;

3.2.85. Deverá possuir a capacidade de controlar o tráfego baseado no Endereço MAC, Frame types, Tipos de Protocolos, Endereços IP e intervalo de portas;

3.2.86. Deverá possuir a capacidade de controlar conexões TCP baseado nas Flags TCP;

3.2.87. Deverá possuir a capacidade de definir regras distintas para interfaces de rede distintas;

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

3.2.89. Deverá possuir a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;

3.2.90. Deverá possuir a capacidade de definição de regras para contextos específicos;

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

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

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

3.2.94. O firewall deverá ser stateful bidirecional;

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

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

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

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

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

3.2.100. Deverá realizar pseudo stateful em tráfego UDP;

3.2.101. Deverá logar a atividade stateful;

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

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

3.2.104. Deverá prevenir ack storm;

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

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

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

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

3.2.109. Deverá oferecer recursos para proteção contra Vulnerabilidades de Sistemas Operacionais e Aplicações;

3.2.110. Deverá possuir a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;

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

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

3.2.113. Deverá possuir a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão;

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

3.2.115. Deverá possuir a capacidade de armazenamento do pacote capturado quando detectado um ataque;

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

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

3.2.118. Deverá possuir a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injection e Cross Site Scripting. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;

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

3.2.120. A solução deverá possuir a capacidade de permitir ou negar que métodos utilizados por Webservers por regras de IPS;

3.2.121. Deverá permitir que regras de IDS/IPS possam ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não) ou poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

3.2.122. Deverá ser capaz de inspecionar tráfego criptografado de entrada;

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

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

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

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

3.2.127. Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de uma determinada web browser ou aplicação de backup;

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

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

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

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

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

3.2.133. As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta;

3.2.134. As regras deverão ser atualizadas automaticamente pelo fabricante;

3.2.135. Deverá possuir a funcionalidade de atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas;

3.2.136. Monitoramento De Integridade para Servidores

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

3.2.138. Deverá possuir a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;

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

3.2.140. Deverá possuir a capacidade de monitorar o status de serviços e processos do sistema operacional;

3.2.141. Deverá possuir a capacidade de monitorar mudanças efetuadas no registro do Windows;

3.2.142. Deverá possuir a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e customização de XML para criação de regras avançadas;

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

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

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

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

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

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

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

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

3.2.151. Deverá possuir capacidade de Inspeção de Logs para Servidores

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

3.2.153. Deverá possuir a capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos;

3.2.154. Deverá possuir a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de inspeção de logs de

acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;

3.2.155. Deverá permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;

3.2.156. Deverá permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;

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

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

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

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

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

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

3.2.163. As regras deverão se atualizar automaticamente pelo fabricante;

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

3.2.165. Deverá possuir capacidades de Controle De Aplicações

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

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

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

3.2.169. A console deverá exibir eventos de no mínimo 30 dias;

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

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

3.2.172. Deverá possuir funcionalidades de Detecção e Resposta;

3.2.173. solução deverá possuir módulo de investigação, detecção integrados;

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

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

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

3.2.177. O módulo de detecção e resposta deverá atuar baseado em modelos de detecção de ataques avançados e furtivos;

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

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

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

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

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

3.2.183. Deverá permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;

3.2.184. Deverá permitir o envio de notificações para os administradores através de e-mail, API e integrações com SIEMs;

3.2.185. Deverá prover visualização em linha do tempo com informações dos eventos monitorados em cada servidor;

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

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

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

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

3.2.190. A solução deverá por meio de agente único possibilitar a conexão com a plataforma de detecção e resposta do próprio fabricante de maneira nativa sem a necessidade de plug-ins ou agentes adicionais;

3.2.191. Esta conexão deverá garantir, sem qualquer configuração local, que o sensor de detecção e resposta esteja ativo e envie telemetria a plataforma;

3.3. Console de gerenciamento da plataforma de detecção e resposta estendida

3.3.1. A solução deve fornecer uma console única para gerenciamento dos serviços de segurança, integrando-se com os outros componentes;

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

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

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

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

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

3.3.7. Deverá orquestrar todas as funcionalidades descritas;

3.3.8. A solução deverá permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob demanda, ou por tarefa agendada com o envio automático do relatório por e-mail;

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

3.3.10. Prover nota de risco para o ambiente de TI da CONTRATANTE, baseada em diversos fatores e comparável com a de outras organizações da mesma região, indústria ou tamanho;

3.3.11. Deve suportar integração com os seguintes serviços de diretório:

3.3.11.1. Microsoft Active Directory;

3.3.11.2. Azure Active Directory;

3.3.11.3. Open LDAP;

3.3.12. A nota de risco deve ser calculada continuamente e deve ser possível analisar seu comportamento ao longo do tempo de forma gráfica;

3.3.13. As fontes de dados para cálculo do risco não devem se limitar àquelas desenvolvidas pelo FABRICANTE, sendo aceitas soluções de terceiros;

3.3.14. Deve prover um sumário dos itens referentes ao escopo de risco cibernético mapeado, apresentando as ações a serem executadas, a fim de diminuir o valor numérico do risco;

3.3.15. Deve apresentar alertas de possíveis comprometimentos de contas;

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

3.3.17. Suporte a atribuição de papéis funcionais, para implantação de política de controle de acesso baseada em papéis (RBAC - Role-based access control);

3.3.18. A console de administração deve metrificar o nível de risco cibernético do ambiente, baseando-se na telemetria gerada pelas demais funcionalidades e características citadas neste documento;

3.3.19. Deve mapear as vulnerabilidades existentes nas máquinas, elencando quanto ao nível de CVSS score e impacto no ambiente, apresentando as vulnerabilidades que estão sofrendo algum tipo de exploração a nível das máquinas e da rede;

3.3.20. Deve apontar as vulnerabilidades com o maior índice de risco presentes no ambiente;

3.3.21. Deve apresentar os alertas de ameaças direcionadas, suspeitas, e de dia zero, a fim de identificar possíveis ações maliciosas no ambiente da CONTRATANTE;

3.3.22. Tais alertas devem apresentar:

3.3.22.1. A relação entre máquinas e IPs;

3.3.22.2. Requisições de rede;

3.3.22.3. URLs e Hashs;

3.3.22.4. Usuários e domínios;

3.3.23. Deve ser possível customizar os modelos de detecção, a fim de atender as necessidades da CONTRATANTE;

3.3.24. Deve ser possível criar exceções para os modelos de detecção;

3.3.25. A solução deve ser baseada em inteligência artificial e aprendizagem de máquina, a fim de potencializar os níveis de detecção de comportamentos anômalos;

3.3.26. Deve possuir rede global de inteligência de ameaças;

3.3.27. Deve apresentar alertas caso os dados de telemetria gerados tenham relação com algum tipo de campanha de ameaças globais;

3.3.28. Deve possuir módulo de pesquisa forense de ameaças, possibilitando a coleta de logs remotamente;

3.3.29. Deve suportar conexões remotas via agente da solução, sendo possível:

3.3.29.1. Coleta de evidências forenses;

3.3.29.2. Isolar a máquina;

3.3.29.3. Terminar processo;

3.3.29.4. Dump de memória;

3.3.29.5. Listar as portas abertas na máquina;

3.3.29.6. Listar configurações de rede;

3.3.29.7. Listar os diretórios;

3.3.29.8. Deletar arquivo ou diretório;

3.3.30. A solução deverá possibilitar enumerar a superfície de ataque da CONTRATANTE, dependendo das fontes de dados conectadas, compreendendo:

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

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

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

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

3.3.30.5. Os domínios da CONTRATANTE, suportando ao menos 10 domínios diferentes;

3.3.30.6. Os subdomínios da CONTRATANTE;

3.3.30.7. Os IPs Públicos associados à CONTRATANTE e seus respectivos hosts;

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

3.3.30.9. Deve mapear via rede da CONTRATANTE os dispositivos existentes e apontar aqueles que não são gerenciados pelos agentes da solução.

3.3.31. Deverá apresentar a relação de máquinas que o usuário acessou;

3.3.32. Deverá listar os alertas identificados no ambiente e correlacionar com técnicas, táticas e procedimentos do framework MITRE ATT&CK;

3.3.33. Tais alertas devem seguir o seguinte escopo de severidade quanto ao nível de risco:

3.3.33.1. Risco Crítico;

3.3.33.2. Risco Alto;

3.3.33.3. Risco Médio;

3.3.33.4. Risco Baixo.

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

3.3.35. Deverá haver correlação entre eventos de detecção, a fim de apresentar um possível incidente de segurança;

3.3.36. Deverá suportar que o usuário manualmente correlacione alertas em um incidente;

3.3.37. Deverá possibilitar que um usuário atribua o alerta a outro usuário;

3.3.38. Deverá possuir campo para observações e notas;

3.3.39. Cada alerta deverá ser listado com um status de:

3.3.39.1. Novo alerta;

3.3.39.2. Alerta sendo tratado;

3.3.39.3. Falso Positivo

3.3.39.4. Fechado;

3.3.39.5. Verdadeiro Positivo.

3.3.40. Deverá listar todos as ações de resposta executadas, apresentando o status de cada uma;

3.3.41. Deverá possuir lista customizável de indicadores de comprometimento e objetos suspeitos;

3.3.42. Deverá permitir adicionar arquivos SHA-1, SHA-256, URLs, IPs, domínios e endereços de e-mail a lista de objetos suspeitos;

3.3.43. Deverá permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de objetos suspeitos;

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

3.3.45. A solução deverá mostrar, pelo menos, o timestamp e objetos envolvidos (comandos, processos, usuários, servidores);

3.3.46. Ao clicar em quaisquer dos objetos, a solução deverá permitir realizar buscas específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.

3.3.47. Para a integração com o sensor de inspeção de rede, a solução deverá receber os alertas advindos do sensor de inspeção de rede, processá-los e analisá-los, a fim de identificar os riscos de segurança existentes;

3.3.48. Com base na telemetria do sensor de inspeção de rede, deverá replicar a sequência de requisições ocorridas dentre as máquinas da rede da CONTRATANTE e endereços externos, a fim de apresentar eventos correlacionados para permitir investigações forenses;

3.3.49. Deverá correlacionar os logs do sensor de inspeção de rede e indicar quais vulnerabilidades existentes nas máquinas estão sofrendo tentativas de exploração;

3.3.50. A partir da identificação de uma exploração de vulnerabilidade em determinadas máquinas, a solução deverá ser capaz de disponibilizar as regras de proteção indicadas;

3.3.51. Deverá ser capaz de automaticamente enviar as regras de proteção frente as vulnerabilidades por meio da console do gerenciamento e aplicá-las

diretamente no appliance de Prevenção de Intrusão de rede de 2º Geração, sem necessidade de ação manual;

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

3.3.53. Com base na telemetria gerada, deverá apresentar de forma gráfica fases de um possível ataque, por meio das correlações aplicadas;

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

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

3.3.56. Deverá utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;

3.3.57. Deverá apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;

3.3.58. Deverá ser capaz de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;

3.3.59. Deverá possuir a capacidade de construir sequências de buscas para localizar os dados ou objetos no ambiente que será feita a análise;

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

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

3.3.62. Deverá permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;

3.3.63. Deverá consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;

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

3.3.65. A solução deverá reagir programaticamente, por meio de roteiros customizáveis, quando da detecção de alto risco de máquinas presentes no ambiente da CONTRATANTE;

3.3.66. A ação de interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta deverá estar disponível;

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

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

3.3.69. Deverá elencar o nível de risco cibernético dos usuários da CONTRATANTE, identificando os que apresentem comportamentos anômalos de:

3.3.69.1. Comprometimento de credencial;

3.3.69.2. Ataque de força bruta;

3.3.69.3. Login atípico ou impossível;

3.3.69.4. Login via IPs suspeitos;

3.3.69.5. Múltiplas tentativas de login com sucesso e insucesso.

3.3.70. A partir da dos alertas de risco dos usuários, deverá ser possível enviar ações de mitigação de risco:

3.3.70.1. Forçar reset de senha;

3.3.70.2. Desabilitar conta do usuário no serviço de diretório;

3.3.70.3. Forçar sign-out do usuário.

3.3.71. Deverá centralizar as ações e estender a visibilidade sob todas as funcionalidades, sendo elas:

3.3.71.1. Inspeção de rede contra ameaças avançadas com detecção e resposta;

3.3.71.2. Detecção e resposta para Servidores e cargas de trabalho;

3.3.71.3. Detecção e resposta para estações de trabalho;

3.3.71.4. Controle de acesso a aplicações internas, externas e na nuvem;

3.3.71.5. Prevenção de Intrusão de rede.

3.3.72. A solução deverá prover relatórios contendo no mínimo as seguintes informações:

3.3.72.1. Top Ameaças;

3.3.72.2. Top usuários com risco;

3.3.72.3. Top vulnerabilidades identificadas;

3.3.72.4. Top Hosts com detecções;

3.3.72.5. Sumário de tráfego de rede inspecionado.

4. IMPLANTAÇÃO

4.1. A execução da implantação da solução será de total responsabilidade da CONTRATADA;

4.2. A implantação deverá abranger as atividades referentes ao planejamento, instalação e configuração de toda a solução, conforme requerimentos da CONTRATANTE e recomendações do fabricante da solução ofertada;

4.3. Entende-se por:

4.3.1. Planejamento: compreende o levantamento detalhados das informações do ambiente da CONTRATADA para definição dos serviços de instalação e configuração da solução, visando correto planejamento para a implementação da solução ofertada pela CONTRATANTE;

4.3.2. Instalação: compreende a instalação de todos os componentes de softwares e hardware que compõem a solução de acordo com as especificações do fabricante;

4.3.3. Configuração: compreende a configuração e parametrização de todos os softwares e hardwares que compõem a solução de acordo com as especificações do fabricante de modo a atender o especificado neste documento;

4.4. Caberá à CONTRATADA todo o processo de planejamento, instalação, configuração e testes da solução, que deverá ser integrada à infraestrutura de

tecnologia de informação existente no ambiente da CONTRATANTE, sem impacto significativo a operação;

4.5. Caberá à CONTRATADA a obrigatoriedade de fornecer, instalar e configurar, a critério exclusivo da CONTRATANTE, as atualizações e correções de todos os softwares fornecidos, sem ônus adicionais à CONTRATANTE, durante o período de vigência do contrato;

4.6. Para a execução dos serviços de implantação e migração ora especificados, a CONTRATADA deverá apresentar sua equipe de trabalho, composta pelo gestor de projeto e sua equipe técnica, na data da primeira reunião de acompanhamento da execução do contrato (Kick off), a ser acordada entre a CONTRATANTE e a CONTRATADA e no prazo máximo de 5 dias úteis, após a emissão da OS;

4.7. O gestor do projeto deverá ser um profissional graduado de nível superior (nível sênior) com experiência em gerenciamento de instalação de projetos de infraestrutura de tecnologia da informação (TI);

4.8. A equipe técnica deverá ser composta por profissionais especializados, graduados de nível superior com experiência em consultoria de instalação da solução ofertada, visando assegurar a otimização de suas atividades e o fiel cumprimento de suas obrigações decorrentes do contrato, consequente da licitação, a ser comprovado pelo vencedor da licitação através de atestados de conclusão de cursos ou atestados de clientes, onde tenha efetivado implantação pertinente;

4.9. A equipe técnica deverá assumir um papel chave em prover experiência para as iniciativas táticas e estratégicas da CONTRATANTE. Este esforço deverá incluir as seguintes atividades:

4.9.1. Levantamento detalhado das informações do ambiente e definição das parametrizações da solução necessárias à CONTRATANTE;

4.9.2. Planejamento da instalação, configuração e migração necessária para a adequada implantação da solução;

4.9.3. Validação da matriz de compatibilidade para com o ambiente existente;

4.9.4. Instalação dos produtos em sua totalidade e de acordo com o planejamento definido;

4.9.5. Proporcionar a passagem de conhecimento e melhores práticas ao grupo de administradores de sistemas da CONTRATANTE;

4.9.6. Suporte à operação da solução oferecida durante o período de instalação, quando solicitado pela CONTRATANTE;

4.9.7. O prazo máximo para a execução dos serviços de implantação dos produtos será de 30 dias úteis a contar da emissão da OS;

4.10. Os serviços de implantação deverão ser executados pela CONTRATADA no site da CONTRATANTE, Rua Zuma de Sá Fernandes, 360 – Presidente Altino – Osasco - SP, ou em caso necessário, em outro endereço, desde que no âmbito da região metropolitana de São Paulo;

4.11. Os serviços de implantação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8 e 17 horas, de segunda a sexta-feira, devendo eventualmente, atender à CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de implementações que necessitem ser executados nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente, e de comum acordo entre as partes;

4.12. Caberá à CONTRATADA a integração dos produtos da solução ofertada à infraestrutura de tecnologia da informação existente no local de instalação da CONTRATANTE, respeitando-se as compatibilidades;

4.13. A equipe técnica da CONTRATADA que irá executar a instalação deverá trabalhar sob orientação e supervisão direta do profissional responsável pela coordenação das atividades de instalação (Gestor do projeto);

4.14. Toda informação manuseada pela CONTRATADA são de uso exclusivo e restrito da CONTRATANTE. A CONTRATADA deverá assumir compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários da CONTRATANTE e quaisquer outras informações pertencentes à CONTRATANTE;

4.15. A CONTRATADA, após concluído o serviço de instalação e configuração da solução no site CONTRATANTE, deverá realizar, com o acompanhamento dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi instalada

de acordo com o cenário requerido pela CONTRATANTE e conforme definido no plano de trabalho;

4.16. Escopo da instalação:

4.16.1. Deverão ser instalados todos os softwares e hardwares da solução necessários para atender ao especificado pela CONTRATANTE neste termo de referência;

4.16.2. Integração da solução com o ambiente da CONTRATANTE;

4.16.3. Configuração dos produtos de acordo com os parâmetros técnicos especificados pela CONTRATANTE;

4.16.4. A CONTRATADA deverá habilitar as licenças e os softwares fornecidos;

4.16.5. A CONTRATADA deverá realizar testes de validação da instalação da solução;

4.16.6. A CONTRATADA deverá elaborar e entregar para a equipe da CONTRATANTE a documentação completa do ambiente implementado;

4.16.7. A CONTRATADA deverá prestar apoio à configuração dos equipamentos que caracterizem adequação das instalações ou melhoria no desempenho, em termos de segurança, produtividade, contingência ou outros benefícios. Isto poderá ocorrer por iniciativa de ambas as partes, sempre com anuência da CONTRATANTE;

4.16.8. A CONTRATADA deverá prestar apoio para a reinstalação e/ou reconfiguração dos equipamentos em ocorrências de problemas dos recursos cobertos por garantia;

5. RELATÓRIOS

5.1. A CONTRATADA deverá entregar, para validação da CONTRATANTE, pelo menos dois relatórios com conteúdo definidos a seguir:

5.1.1. Relatório de projeto de implantação:

5.1.1.1. Contempla-se neste relatório, a etapa de planejamento para a implantação da solução especificada neste documento;

5.1.1.2. Neste relatório deverá constar a relação completa dos softwares e hardwares a serem fornecidos, discriminando detalhadamente a finalidade de cada um;

5.1.1.3. O relatório deverá contemplar e detalhar todas as etapas da instalação, isto é, os serviços de planejamento, instalação, configuração e pré- operação;

5.1.1.4. O relatório deverá contemplar cronograma informando o prazo para a execução de cada etapa do serviço contemplado neste relatório;

5.1.1.5. O relatório deverá contemplar a arquitetura desenhada pela CONTRATADA para a integração da solução, na estrutura existente na CONTRATANTE;

5.1.1.6. O prazo máximo para a entrega do relatório de projeto de implantação pela CONTRATADA à CONTRATANTE é de 10 dias úteis a contar da data da primeira reunião de acompanhamento da execução do contrato;

5.1.2. Relatório final de implantação:

5.1.2.1. Neste documento deverão constar todas as informações geradas pela CONTRATADA abordando os aspectos da solução implantada, suas configurações e testes no ambiente da CONTRATANTE;

5.1.2.2. O relatório final de implantação deverá ser fornecido no prazo máximo de 15 dias a contar da data de conclusão e validação dos serviços de instalação e configuração especificados;

5.1.2.3. Todos os relatórios serão considerados como efetivamente entregues e aceitos somente após a validação pela equipe técnica da CONTRATANTE que se fará no prazo máximo de 10 dias úteis a contar da respectiva entrega;

5.1.2.4. Os relatórios deverão ser apresentados em via impressa e/ou meio digital;

5.1.2.5. O software empregado na confecção dos textos integrantes das documentações deverá ser totalmente compatível com o MS Word em versão mais recente;

5.1.2.6. Os relatórios deverão ser emitidos em papel timbrado da CONTRATADA e deverão conter o nome, data e assinatura do gestor de projeto da CONTRATADA.

6. SUPORTE TÉCNICO DA SOLUÇÃO

6.1. O suporte técnico contempla toda a vigência contratual a partir da emissão da Ordem de Serviço;

6.2. O suporte técnico a ser prestado pela CONTRATADA tem por objetivo garantir o pleno, correto e seguro funcionamento da solução de CONTRATADA;

6.3. O suporte técnico compreende a perfeita execução da solução, incluindo todos os seus componentes de software e hardware, integrações e atualizações, de forma que o objeto contratado seja operado seguindo os requisitos definidos nesse documento e os procedimentos de melhores práticas de TI;

6.4. O suporte técnico compreende, ainda, a correção de falhas ou inconsistências detectadas, o auxílio na configuração dos componentes da solução para o correto funcionamento, além do esclarecimento de dúvidas dos empregados e prestadores de serviços da CONTRATANTE, de forma a garantir a melhor utilização e maximização dos recursos contratados;

6.5. A CONTRATADA deverá fornecer suporte telefônico (Central de Atendimento) para acionamento, por meio de ligação gratuita (0800) ou local à RMSP de São Paulo, e ferramenta Web (sítio acessível via Internet), 24 horas por dia, para abertura ou acompanhamento dos chamados realizados. A CONTRATADA deverá oferecer serviço de suporte técnico presencial no site da CONTRATANTE, Rua Zuma de Sá Fernandes, 360 – Presidente Altino – Osasco – SP, de segunda à sexta-feira, entre 08h00 e 17h00;

6.6. As solicitações de atendimento técnico partirão CONTRATANTE através do Gestor do Contrato, ou de outro empregado ou área CONTRATANTE designado para tal finalidade, e deverão ser protocoladas em registro próprio da CONTRATADA;

6.7. Para cada solicitação de atendimento técnico, deverá ser gerado um identificador único (protocolo) para fins de controle e acompanhamento. A CONTRATADA deverá informar esse identificador à CONTRATANTE, bem como manter o histórico de ações e atividades nos chamados realizados durante toda a vigência contratual;

6.8. Nas solicitações de atendimento, o colaborador da CONTRATANTE informará:

6.8.1. Nome do solicitante;

6.8.2. Nome do software ou hardware e sua versão;

6.8.3. Relato do problema e seu nível de criticidade;

6.8.4. Outras informações que julgar pertinentes para resolução do problema;

6.9. A Ferramenta Web, a ser disponibilizada pela CONTRATADA, deverá:

6.9.1. Controlar todas as aberturas de chamados técnicos e os níveis de serviço;

6.9.2. Permitir que a CONTRATANTE tenha acesso para efeito de acompanhamento das providências em andamento e do tempo decorrido desde a abertura;

6.9.3. Permitir que cada profissional CONTRATANTE, indicado pelo Gestor do Contrato, seja cadastrado nesse sistema e receba identificação e senha que permita acesso seguro, de maneira a evitar que pessoas não autorizadas possam acionar o serviço;

6.9.4. Permitir a emissão de relatórios gerenciais, de acordo com as demandas da CONTRATANTE, e o acompanhamento sobre cumprimento dos níveis de serviço estabelecidos neste documento, para subsidiar faturamento e eventuais glosas;

6.9.5. Sempre que solicitado, os especialistas técnicos do fabricante da solução ofertada pela CONTRATADA deverão apoiar e/ou atuar na resolução dos incidentes junto ao suporte da CONTRATADA, caso este não seja realizado diretamente pelo fabricante da solução ofertada;

7. ACORDO DE NÍVEL DE SERVIÇO

7.1. Para cada chamado técnico, a CONTRATADA deverá respeitar os prazos regidos no Contrato vigente.

8. ATUALIZAÇÕES E MANUTENÇÕES

8.1. Atualizações tecnológicas

8.1.1. A CONTRATADA deverá notificar a CONTRATANTE sempre que houver novas atualizações da solução ofertada;

8.1.2. A atualização tecnológica inclui o fornecimento a CONTRATANTE de todas as versões, features, releases, fixes, services packs e patches de segurança de todos os elementos da solução CONTRATADA, garantindo a segurança e a confiabilidade requerida e inerente a cada elemento, de acordo com as especificações deste documento, sem quaisquer custos adicionais a CONTRATANTE;

8.1.3. As atualizações deverão ser repassadas CONTRATANTE no prazo máximo de 30 (trinta) dias a partir do seu lançamento, assim como o fornecimento dos

manuais, boletins técnicos e demais informações pertinentes para sua plena utilização;

8.1.4. Na atualização de versões, a CONTRATADA deverá garantir o apoio técnico necessário para instalação e operação das últimas versões, sem custos adicionais para a CONTRATANTE;

8.1.5. Todas as atualizações da solução CONTRATADA deverão ser liberadas em pacotes completos pela CONTRATADA, no repositório definido pela CONTRATANTE, com a devida identificação da versão em prazo hábil, para teste e homologação em ambiente não produtivo da CONTRATANTE. Somente após a devida homologação técnica e negocial, a implantação em produção poderá ser solicitada;

8.1.6. As versões deverão ser liberadas em conjunto com documentação técnica, documentação de instalação e manual do usuário atualizado, conforme alterações contempladas na versão;

8.2. Requisitos de Manutenção

8.2.1. Os procedimentos para a realização das manutenções e suas respectivas implantações deverão estar sob coordenação da CONTRATADA responsável pela manutenção do ambiente da CONTRATANTE, e estar em conformidade com os processos internos da CONTRATANTE;

8.2.2. Os valores referentes às manutenções previstas neste documento deverão estar inclusos na proposta da CONTRATADA. Não havendo custos adicionais.

8.3. Manutenção Preventiva

8.3.1. A manutenção preventiva será destinada a atualizar os componentes do software (atualização tecnológica), conforme definições nesse documento, e a realizar quaisquer operações que evitem uma parada total ou parcial da solução de TI;

8.3.2. A CONTRATANTE, através de sua equipe técnica, observará o desempenho do sistema contratado e, caso necessário, solicitará à CONTRATADA uma manutenção preventiva para viabilizar a melhor performance do sistema;

8.3.3. Durante a manutenção preventiva, a CONTRATADA deverá analisar a solução, sua condição atual de funcionamento, seus logs de sistema e sugerir mudanças

para uma melhor prática de utilização da ferramenta. A equipe técnica da CONTRATANTE decidirá sobre a aplicação ou não das recomendações apresentadas;

8.4. Manutenção Corretiva

8.4.1. A manutenção corretiva será destinada a remover erros ou falhas apresentados pelos componentes de software da ferramenta CONTRATADA;

8.4.2. Como erro ou falha entende-se a geração de resultado diferente do previsto, por parte da CONTRATADA, em decorrência da não observância de regra de negócio ou erros de definição técnica ou de implementação. Para a resolução desses erros, é necessária a intervenção técnica especializada ou mesmo até a substituição de seus componentes por parte da CONTRATADA;

8.4.3. A manutenção corretiva pode ser solicitada a qualquer momento pela CONTRATANTE e está poderá ser fornecida como Patch de correção;

8.4.4. Caso a manutenção corretiva implique em manutenções de sistemas e demais componentes dos ambientes tecnológicos não cobertos pela CONTRATADA e isso gere custos para CONTRATANTE, os valores poderão ser repassados para a CONTRATADA, após o devido processo de apuração de responsabilidade, em forma de glosa nos pagamentos pendentes, a critério da CONTRATANTE.

9. PRAZOS, ENTREGAS E RECEBIMENTOS

9.1. Ordem de serviço, recebimento provisório e definitivo

9.1.1. A emissão da OS ocorrerá em até 5 dias úteis após a data da assinatura do contrato;

9.1.2. O TRP, Termo de Recebimento Provisório e TRD, Termo de Recebimento Definitivo, são documentos constantes no sistema normativo da CONTRATANTE, itens 3.4 e 3.5 da NI.03/001 – Gestão de instrumentos contratuais e art. 163 e itens LI e LII do regulamento de licitações, contratos e demais ajustes;

9.1.3. A CONTRATANTE emitirá o TRP e TRD para os produtos e serviços após a constatação de que o objeto contratual e suas fases atenderam às especificações técnicas requeridas descritas neste Termo de Referência;

9.1.4. Caso os produtos apresentem defeito ou os serviços não atendam às especificações técnicas básicas requeridas, os prazos de recebimento serão reiniciados após a solução dos problemas detectados;

9.1.5. O prazo para a resolução dos problemas mencionados no item 8.1.4 é de 5 dias úteis a contar do comunicado da CONTRATANTE;

9.2. Implantação

9.2.1. O serviço de implantação da solução, item 3, deverá ser concluído em até 30 dias úteis da emissão da OS;

9.2.2. A implantação só será considerada concluída após a emissão do seu TRP, o qual será emitido em até 5 dias úteis após a aferição da conclusão desta fase;

9.2.3. A emissão do TRP, Termo de Recebimento Provisório, item 3.4 da NI.03/001 – Gestão de Instrumentos Contratuais e art. 163 e item LII do Regulamento de Licitações, Contratos e demais ajustes, ocorrerá em até 5 dias úteis após;

9.2.4. A emissão do TRD, Termo de Recebimento Definitivo, item 3.5 da NI.03/001 – Gestão de Instrumentos Contratuais e art. 163 e item LI do Regulamento de Licitações, Contratos e demais ajustes, ocorrerá em até 5 dias úteis após a aferição da conclusão da totalidade do objeto;

10. MEDIÇÃO

10.1. Relatório de medição

10.1.1. Os serviços contratados serão apontados por medições mensais discriminados em relatório e deverão contemplar todos os serviços no período e aprovados pela CONTRATANTE;

10.1.2. As medições deverão indicar as quantidades correspondentes aos serviços prestados;

10.1.3. As medições deverão ser numeradas sequencialmente, discriminando o número do contrato, o seu objeto e o período de abrangência da mesma;

10.1.4. As medições deverão ser apresentadas ao GESTOR até o 5º dia útil, contado do último dia do período de adimplemento de cada obrigação, mediante protocolo que conste a data de sua entrega;

10.1.5. O GESTOR terá o prazo de 5 (cinco) dias úteis para a conferência da medição

e a sua aprovação;

10.1.6. A medição não aprovada pelo GESTOR será devolvida à CONTRATADA para as necessárias correções, com as informações que motivaram a sua rejeição, contando-se o prazo estabelecido no subitem anterior, a partir da data de sua reapresentação;

10.1.7. A devolução da medição não aprovada pelo GESTOR, em hipótese alguma, servirá de pretexto para que a CONTRATADA suspenda a execução dos serviços;

10.1.8. Na hipótese de não pronunciamento pelo GESTOR quanto à medição no prazo definido anteriormente, considerar-se-á aprovada a medição;

11. CONDIÇÕES DE PAGAMENTO

11.1. A CONTRATANTE procederá ao pagamento nas condições previstas nesta cláusula;

11.2. Após a aprovação da medição a CONTRATADA deverá, num prazo de até 02 (dois) dias úteis, apresentar ao departamento fiscal da CONTRATANTE as vias originais da nota fiscal, das quais deverão constar todos os tributos incidentes na fonte sobre a prestação dos serviços, conforme estabelecido na cláusula de tributos descrito no edital, acompanhadas do respectivo documento de cobrança;

11.3. Na nota fiscal e no documento de cobrança deverão ainda ser indicados o número do contrato, o período medido e o número da medição. No processo do pagamento, obedecerá a CONTRATANTE as disposições contidas na Lei nº 8.212, de 24 de julho de 1991, regulamentada pelo Decreto nº 3048, de 06 de maio de 1999 e demais normas pertinentes;

11.4. O documento de cobrança não aprovado pelo GESTOR será devolvido à CONTRATADA para as necessárias correções, com as informações que motivaram sua rejeição, contando-se o prazo estabelecido a partir da data de sua apresentação;

11.5. A CONTRATANTE efetuará o pagamento no prazo de 30 (trinta) dias, a contar do último dia do período de adimplemento de cada parcela, desde que aprovados a medição, nota fiscal e documento de cobrança, nos prazos estabelecidos nas cláusulas de medição e de pagamento;

11.6. Na hipótese de ocorrer a devolução da medição, conforme previsto na correspondente cláusula, o prazo de pagamento será dilatado pelo número de dias contados entre a data de devolução e a (s) data (s) da nova apresentação.

12. EXECUÇÃO DOS SERVIÇOS

12.1. A quantidade estimada de meses após contratação do objeto deste termo é de 14 (quatorze) meses.

.

13. ANEXO I – PLANILHA DE QUANTIDADES E PREÇOS.

Item	Solução/Serviço	Qtde estimada.	Unidade	Custo unitário (R$)	Custo total (R$)
1	Solução de inspeção de rede contra ameaças avançadas com detecção e resposta.	14	Meses		
2	Solução de segurança para servidores e cargas de trabalho híbridas com detecção e resposta.	14	Meses		
3	Console de gerenciamento unificada da plataforma com detecção e resposta estendida para extensão de visibilidade do ambiente e ação imediata contra ameaças.	14	Meses		
4	Serviço de manutenção e suporte	14	Meses		
5	Serviços de implantação e configuração	1	Unidade		
Total					

ANEXO 3

TERMO DE ADITAMENTO Nº 02 AO CONTRATO Nº 072222305100

ESPECIFICAÇÃO DE SERVIÇO E PREÇO ESP E0220920-T01

Prodesp

Governo do Estado de São Paulo
Companhia de Processamento de Dados do Estado de São Paulo
Coordenadoria de Novos Negócios

PROPOSTA

Nº do Processo: 359.00000452/2023-27

Interessado: COMPANHIA PAULISTA DE TRENS METROPOLITANOS-CPTM, Gerência de Segurança da Informação

Assunto: CPTM - Contrato de Prestação de Serviços de Outsourcing de TI - Tecnologia da Informação

Prodesp

Governo do Estado de São Paulo
Companhia de Processamento de Dados do Estado de São Paulo
Coordenadoria de Novos Negócios

PLANILHA DE ORÇAMENTO ESPECIFICAÇÃO DE SERVIÇOS E PREÇOS

ESP - E0220920-T01 PNPP nº 10167.2023

TERMO DE ADITAMENTO E RERRATIFICAÇÃO Nº 01 DA ESPECIFICAÇÃO DE SERVIÇOS E PREÇOS N.º E0220920

Este documento, a partir de sua assinatura, fará parte integrante do Contrato de Prestação de Serviços **PD022474,** firmado com a **COMPANHIA PAULISTA DE TRENS METROPOLITANOS - CPTM.**

1. **OBJETO**

O presente termo tem por finalidade de: **INCLUIR** os subitens **"2.7. Implementação de novas camadas de Proteção Trend Micro Apex One", "2.8. Serviço de Inspeção Avançada de Tráfego de Redes - 360°", "2.9. Serviço de Proteção para *Workloads" e "*2.10. Serviço de Análise de Logs e Informações para Correlação de Eventos"** no item **"2. ESCOPO DA PRESTAÇÃO DE SERVIÇOS"**, bem como, **RATIFICAR** o caput do item **"5. PREÇOS E CONDIÇÕES DE PAGAMENTO",** descrito na Especificação de Serviços e Preços original.

2. **ADITAMENTO E RERRATIFICAÇÃO**

Em razão do presente termo, **a partir da data de assinatura**, os subitens **"2.7. Implementação de novas camadas de Proteção Trend Micro Apex One", "2.8. Serviço de Inspeção Avançada de Tráfego de Redes - 360°" , "2.9. Serviço de Proteção para *Workloads" e "*2.10. Serviço de Análise de Logs e Informações para Correlação de Eventos"** passam a fazer parte do item **"2. ESCOPO DA PRESTAÇÃO DE SERVIÇOS"** e o item **"5. PREÇOS E CONDIÇÕES DE PAGAMENTO"** da Especificação de Serviços e Preços original, passam a vigorar com a seguinte redação:

"*2. ESCOPO DA PRESTAÇÃO DE SERVIÇOS*

Fica acrescentado o seguinte escopo:

2.7. IMPLEMENTAÇÃO DE NOVAS CAMADAS DE PROTEÇÃO

TREND MICRO APEX ONE

2.7.1. Plataforma como Serviços – PaaS Middleware com Serviços de Gestão de Middleware

Este serviço disponibiliza os softwares necessários para continuidade dos serviços implantados na **s o l u ç ã o** da CONTRATANTE e para garantir o correto funcionamento das plataformas, bem como a troca de dados de forma segura entre seus diversos módulos. Estão excluídos deste item os serviços de Plataforma de Banco de Dados (PaaS Oracle e PaaS SQL), bem como os serviços de Plataforma de Aplicações (PaaS JBOSS e PaaS Websphere.

2.7.1.1 Atividades previstas

Estão contemplados os seguintes softwares:

§ 1 Renew Deep Discovery Inspector Series 4000 4 Gbps;
§ 300 Trend Micro Cloud One Workload Security;
§ 190.000 XDR / Vision One – Subscription for Trend Micro Vision One Créditos.

2.7.1.2. Serviços Gestão de *Middleware* Básico

·Relatórios de justificativas e aprovações internas;
·Controles de vigência dos licenciamentos;
·Renovações e disponibilidade do licenciamento contratado junto ao fornecedor;
·Controles e medições das licenças disponibilizadas no portal do fornecedor;
·Gestão de novas demandas com o fornecedor;
·Gestão de Fornecedores;
·Orientação e apoio técnico quanto a ativação local e instalação;
·Orientação técnica remota quando necessário;
·Apoio técnico na gestão de usuários e atribuição de licenciamento;
·Apoio técnico no tratamento de incidentes / Troubleshooting;
·Construção e gerenciamento de grupos de usuários para controle de acessos;
·Métricas de uso;
·Ativação e desativação de recursos.

2.7.1.3. Serviços fora do escopo

·Desenvolvimento e manutenção de aplicativos e sistemas;
·Suporte aos usuários dos sistemas utilizados pela CONTRATANTE;
·Gerenciamento, monitoramento, manutenção e suporte à infraestrutura e aos usuários locais no ambiente de TIC.”

2.8. **Serviço de Inspeção Avançada de Tráfego de Redes - 360°**

·Atividades
- o Implantação, suporte e atualização de solução de segurança para inspeção de tráfego de rede físico e virtual, portas e protocolos de rede. Contempla a identificação de malwares avançados, ransomware, explorações de zero-day, comando e controle das comunicações (C&C) e atividades evasivas.

·Melhorias
- o Prevenção, detecção e resposta a incidentes de segurança, através de inspeção de todo o conteúdo da rede, múltiplas técnicas de detecção com machine learning e análise de sandbox personalizada. Permite a detecção de malwares, comportamentos e comunicações invisíveis às defesas tradicionais. Possibilita resposta rápida por meio de inteligência compartilhada de ameaças e entrega de atualizações de segurança em tempo real.

2.9. **Serviço de Proteção para *Workloads***

·Atividades

- Implantação, suporte e atualização de solução de proteção para workloads, compatível com sistemas operacionais Windows e Linux e ambiente de virtualização VMware. Contempla a instalação de agentes para detecção e proteção contra vulnerabilidades, malwares, URLs maliciosas ou de baixa reputação, firewall de host, blindagem de vulnerabilidades de sistemas operacionais e aplicações, inspeção de logs, controle de aplicações, além de mudanças não autorizadas em ambientes físicos e virtuais.

·Melhorias

- Conjunto completo de recursos de segurança através de um único agente. Possui proteção proativa contra ameaças de rede com prevenção de intrusões e Firewall. Proteção contra vulnerabilidades através de virtual patching. Permite o bloqueio de sistemas e recebimento de alertas sobre mudanças não planejadas no sistema com controle de aplicações, monitoramento de integridade e inspeção de logs.

2.10. **Serviço de Análise de Logs e Informações para Correlação de Eventos**

·Atividades

- Implantação, suporte e atualização de plataforma para detecção e resposta a ameaças. Contempla a centralização de informações e logs para correlação de eventos coletados através de soluções de inspeção de rede física e virtual, além de agentes de proteção para workloads, usuários e estações de trabalho. Elaboração de relatórios listando ativos e usuários vulneráveis.

·Melhorias

- Integração com outras ferramentas e tecnologias de segurança existentes no ambiente. Fornece uma fonte centralizada de alertas priorizados para correlacionar e analisar dados, permitindo a visualização de toda a cadeia de eventos nas camadas de segurança, aprofundar em um perfil de execução ou análise de tráfego de rede. Permite a tomada de ações de contenção para endpoints e workloads de forma centralizada."

Em decorrência dessas alterações, o item **"5. PREÇO E CONDIÇÕES DE PAGAMENTO"** passa a vigorar com a seguinte redação:

"5. PREÇOS E CONDIÇÕES DE PAGAMENTO

O preço para a execução dos serviços constantes desta ESP é estimado em **R$ 52.592.478,35** (cinquenta e dois milhões, quinhentos e noventa e dois mil, quatrocentos e setenta e oito reais e trinta e cinco centavos), tendo como data base de referência o mês de **novembro/2022** e será reajustado de acordo com as condições estabelecidas no contrato a que se vincula.

ITEM	DESCRIÇÃO DOS SERVIÇOS	PARCELA ÚNICA	VALOR MENSAL	TOTAL PREVISTO	ADITAMENTO
5.1	ATENDIMENTO E SUPORTE AO USUÁRIO DE TI	R$ -	R$ 133.727,04	R$ 4.011.811,20	R$ -
5.2	SUPORTE LOCAL	R$ -	R$ 300.901,44	R$ 9.027.043,20	R$ -
5.3	GERENCIAMENTO DE SEGURANÇA	R$ -	R$ 108.853,74	R$ 3.265.612,20	R$ -
5.4	GESTÃO E OPERAÇÃO DO AMBIENTE DE TI	R$ 164.568,40	R$ 42.460,72	R$ 1.438.390,00	R$ -
5.5	GESTÃO DE SERVIDORES E ARMAZENAMENTO, E APOIO A BANCO DE DADOS	R$ -	R$ 937.392,62	R$ 28.121.778,60	R$ -
5.6	Implementação de novas camadas de Proteção ao Trend Micro Apex One (ADITAMENTO)	R$ 2.192.893,74	R$ 323.924,96	R$ 6.727.843,15	R$ 6.727.843,15
TOTAL		R$ 2.357.462,14	R$ 1.847.260,52	R$ 52.592.478,35	R$ 6.727.843,15

Todos os subitens serão faturados mensalmente de acordo com as quantidades apuradas no fim de cada mês, com exceção do subitem 5.4 que será faturado mediante parcela única após a execução do serviço.
O subitem 5.6 (aditado), a primeira parcela será única e as restantes mensal fixas.
Serão emitidas Notas Fiscais Eletrônicas e enviadas, automaticamente, pelo sistema das Prefeituras (Taboão da Serra e São Paulo), sendo que para os serviços prestados em Taboão da Serra, serão encaminhadas para o e-mail cadastrado no sistema de contratos da Prodesp, e para os serviços prestados em São Paulo, para o e-mail cadastrado junto àquela Prefeitura.
Recebidas as Notas-Fiscais Eletrônicas, a CONTRATANTE terá o prazo de 03 (três) dias para atestação da execução dos serviços ou devolução para esclarecimentos e correções necessárias.
Os pagamentos deverão ser efetuados dentro do prazo de 30 (trinta) dias da data de apresentação das Notas-Fiscais Eletrônicas."

3. RATIFICAÇÃO

Ficam ratificados todos os demais itens da Especificação de Serviços e Preços original, bem como de seus termos subsequentes, os quais não colidam com o presente termo:

ÁREA DE NEGÓCIOS

Nome : Kelly Cristine da Silva
Endereço: Rua Agueda Gonçalves, 240 - 2º Andar – Lado Par - Jardim Pedro Gonçalves - Taboão da Serra – SP.
Telefone : (011)
2868-3124 E-mail :
ksilva@sp.gov.br

ÁREAS RESPONSÁVEIS PELA EXECUÇÃO DO SERVIÇO

Nome : Paul Haro
Endereço: Rua Agueda Gonçalves, 240 – PD.6.5 – Jardim Pedro Gonçalves - Taboão da Serra – SP.
Telefone : (11) 2845-6000
E-mail : pmharo@sp.gov.br

De acordo

CONTRATANTE

Nome:

Cargo:

Emissão: 03/05/2024

oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Kelly Cristine Da Silva Ferreira**, **Coordenador**, em 09/05/2024, às 16:50, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

A autenticidade deste documento pode ser conferida no site https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0027018864** e o código CRC **D5287A05**.

Governo do Estado de São Paulo
Companhia Paulista de Trens Metropolitanos
Depto De Contratacoes E Compras

TERMO ADITIVO

ANEXO 4

TERMO DE ADITAMENTO Nº02 AO CONTRATO Nº 072222305100

TERMO DE CIÊNCIA E DE NOTIFICAÇÃO

CONTRATANTE: COMPANHIA PAULISTA DE TRENS METROPOLITANOS – CPTM
CONTRATADA: COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO - PRODESP
CONTRATO Nº (DE ORIGEM): 072222305100 – TERMO DE ADITAMENTO Nº 02
OBJETO: PRESTAÇÃO DE SERVIÇOS ESPECIALIZADOS EM TI – TECNOLOGIA DA INFORMAÇÃO, QUE SE CONSTITUEM DE UMA SOLUÇÃO GLOBAL AO AMBIENTE DE TI, A SABER: ATENDIMENTO E SUPORTE AO USUÁRIO DE TI E SERVIÇOS NO AMBIENTE DE TI.
ADVOGADO (S)/Nº OAB/e-mail: CAIO AUGUSTO DE MORAES FORJAZ / OAB Nº 182.311 / e-mail: caio.forjaz@cptm.sp.gov.br e RAFAEL TONIATO MANGERONA / OAB Nº 213.777 / e-mail: rafael.mangerona@cptm.sp.gov.br.

Pelo presente TERMO, nós, abaixo identificados:

1. Estamos CIENTES de que:

a) o ajuste acima referido, seus aditamentos, bem como o acompanhamento de sua execução contratual, estarão sujeitos a análise e julgamento pelo Tribunal de Contas do Estado de São Paulo, cujo trâmite processual ocorrerá pelo sistema eletrônico;

b) poderemos ter acesso ao processo, tendo vista e extraindo cópias das manifestações de interesse, Despachos e Decisões, mediante regular cadastramento no Sistema de Processo Eletrônico, em consonância com o estabelecido na Resolução nº 01/2011 do TCESP;

c) além de disponíveis no processo eletrônico, todos os Despachos e Decisões que vierem a ser tomados, relativamente ao aludido processo, serão publicados no Diário Oficial do Estado, Caderno do Poder Legislativo, parte do Tribunal de Contas do Estado de São Paulo, em conformidade com o artigo 90 da Lei Complementar nº 709, de 14 de janeiro de 1993, iniciando-se, a partir de então, a contagem dos prazos processuais, conforme regras do Código de Processo Civil;

d) as informações pessoais dos responsáveis pela contratante estão cadastradas no módulo eletrônico do "Cadastro Corporativo TCESP – CadTCESP", nos termos previstos no Artigo 2º das Instruções nº01/2020, conforme "Declaração(ões) de Atualização Cadastral" anexa (s);

e) é de exclusiva responsabilidade do contratado manter seus dados sempre atualizados.

2. Damo-nos por NOTIFICADOS para:

a) O acompanhamento dos atos do processo até seu julgamento final e consequente publicação;

b) Se for o caso e de nosso interesse, nos prazos e nas formas legais e regimentais, exercer o direito de defesa, interpor recursos e o que mais couber.

AUTORIDADE MÁXIMA DO ÓRGÃO/ENTIDADE:

Nome: PEDRO TEGON MORO

Cargo: Diretor Presidente

CPF: 144.051.718-58

RESPONSÁVEIS PELA HOMOLOGAÇÃO DO CERTAME OU RATIFICAÇÃO DA DISPENSA/INEXIGIBILIDADE DE LICITAÇÃO:

Nome: x-x-x-x-x-x-x-x
Cargo: x-x-x-x-x-x-x-x
CPF: x-x-x-x-x-x-x-x-x
Assinatura: x-x-x-x-x-x-x-x-x

RESPONSÁVEIS QUE ASSINARAM O AJUSTE:
Pelo contratante:

Nome: ANA CAROLINE DE FARIA EDUARDO BORGES

Cargo: Diretora Administrativa e Financeira

CPF: 003.938.371-73

Nome: PEDRO TEGON MORO

Cargo: Diretor Presidente

CPF: 144.051.718-58

Nome: JOSÉ LUIZ BARCI NEVES
Cargo: Gerente de Tecnologia da Informação
CPF: 853.555.507-20

Pela contratada:
Nome: FERNANDO HIDEYO YOKEMURA
Cargo: Diretor de Operações
CPF: 517.724.930-15

Nome: RAFAEL ALMEIDA FERNANDEZ SOTO
Cargo: Diretor de Desenvolvimento e Sistemas
CPF: 010.570.755-40

RESPONSÁVEL POR AÇÕES DE COORDENAÇÃO, ACOMPANHAMENTO, MONITORAMENTO, AVALIAÇÃO E FISCALIZAÇÃO:
Gestor do contrato:
Nome: JOSÉ LUIZ BARCI NEVES
Cargo: Gerente de Tecnologia da Informação
CPF: 853.555.507-20

ORDENADOR DE DESPESAS DA CONTRATANTE:
Nome: PEDRO TEGON MORO
Cargo: Diretor Presidente
CPF: 144.051.718-58

sei! assinatura eletrônica	Documento assinado eletronicamente por **Rafael Almeida Fernandez Soto**, **Diretor**, em 10/05/2024, às 17:44, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.
sei! assinatura eletrônica	Documento assinado eletronicamente por **Fernando Hideyo Yokemura**, **Diretor**, em 10/05/2024, às 18:00, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.
sei! assinatura eletrônica	Documento assinado eletronicamente por **Jose Luiz Barci Neves**, **Gerente**, em 10/05/2024, às 18:05, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Ana Caroline de Faria Eduardo Borges**, **Diretor**, em 10/05/2024, às 18:22, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Pedro Tegon Moro**, **Diretor Presidente**, em 10/05/2024, às 19:34, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

A autenticidade deste documento pode ser conferida no site https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0027636093** e o código CRC **4AC3C167**.