Data de Emissão: 24/09/2020 13:13:13

REQUISIÇÃO DE MATERIAL - RM - COM PRESTAÇÃO DE SERVIÇO
No.: 20200007 DATA DA RM: 07/01/2020

N.º COLETA: CP-20200015
LISTAGEM No.: 13324

PROGRAMA(S) DE TRABALHO: 03610206101411648

ORGÃO FISCAL: 8616 - DGTEC - DIVISAO DE REDES

PROCESSO: 2020617549
TIPO: VALOR TOTAL

OBJETO: SENSORES DE PREVENÇÃO DE INTRUSÃO (IPS)

PROCEDIMENTO ADOTADO: LICITAÇÃO

ITEM	CÓD. MATERIAL	NOME DO MATERIAL	UF	QTDE	PREÇO	VALOR
1	7440-656-1368-2	SOLUÇÃO IPS	UN	1,000	2.315.312,67	2.315.312,67

EXCLUSIVIDADE

DESCRIÇÃO DO MATERIAL

ESPECIFICAÇÃO CONFORME TERMO DE REFERÊNCIA:

4. ESPECIFICAÇÃO TÉCNICA "

4.1 REQUISITOS INTERNOS

4.1.1 ARQUITETURA DA SOLUÇÃO

4.1.1.1 A SOLUÇÃO DE IPS (INTRUSION PREVENTION SYSTEM) DEVERÁ SER FORNECIDA NA FORMA DE APPLIANCE FÍSICO E DEVERÁ VIR ACOMPANHADA DE:
4.1.1.1.1 CONECTORES E CABEAMENTO NECESSÁRIO PARA A IMPLANTAÇÃO;
4.1.1.1.2 DASHBOARD DE GERENCIAMENTO E CONTROLE.

4.1.1.2 A SOLUÇÃO DEVE POSSUIR UMA ARQUITETURA ESPECÍFICA DESENVOLVIDA PARA A FINALIDADE DE NEXT GENERATION INTRUSION PREVENTION SYSTEM (NGIPS);
4.1.1.3 NÃO SERÃO ACEITAS SOLUÇÕES COM SOFTWARE E HARDWARE DE FABRICANTES DISTINTOS, OU MESMO SOLUÇÕES DE USO GERAL COMO, SERVIDORES, ESTAÇÕES DE TRABALHO OU EQUIPAMENTOS COMO BLADES.
4.1.1.4 A SOLUÇÃO DEVERÁ SER COMPOSTA DE 2 (DOIS) EQUIPAMENTOS DEDICADOS À INSPEÇÃO DO TRÁFEGO PODENDO, A APLICAÇÃO DE GERENCIAMENTO, SER FORNECIDA DE FORMA VIRTUAL.
4.1.1.5 A SOLUÇÃO DE IPS NÃO PODERÁ TER SEU FIM DE VENDA (END-OF-SALE) E FIM DE VIDA (END-OF-LIFE) ANUNCIADO NO MOMENTO DO ACEITE DEFINITIVO DE SUA ENTREGA. CASO SEJA ESSA A SITUAÇÃO, O FORNECEDOR DEVERÁ ENTREGAR UM MODELO EQUIVALENTE OU SUPERIOR AO QUE ENTROU EM FIM DE VENDA E/OU FIM DE VIDA.
4.1.1.6 EM CASO DE ANÚNCIO DO FIM DE VENDA E/OU FIM DE VIDA OCORRER APÓS O ACEITE DEFINITIVO DA ENTREGA DA SOLUÇÃO DE IPS, O FIM DE SUPORTE (END-OF-SUPPORT) NÃO PODERÁ OCORRER NOS PRÓXIMOS 60 (SESSENTA MESES).
4.1.1.7 TODOS OS COMPONENTES DA SOLUÇÃO (HARDWARES E SOFTWARES) DEVERÃO SER FORNECIDOS COM TODAS AS LICENÇAS NECESSÁRIAS AO SEU PLENO FUNCIONAMENTO DE MODO A REALIZAR TODAS AS FUNCIONALIDADES DESCRITAS NESTE TERMO DE REFERÊNCIA.
4.1.1.7.1 AS LICENÇAS A QUE SE REFERE O ITEM 4.1.1.6 DEVERÃO TER CARÁTER PERPÉTUO, NÃO PRECISANDO DE RENOVAÇÃO, DEVENDO SUA ATUALIZAÇÃO (SUBSCRIPTION) SER GARANTIDA PELO PRAZO DO CONTRATO.

4.1.2 DA ALTA DISPONIBILIDADE.

4.1.2.1 A SOLUÇÃO DEVE SER ESCALÁVEL PARA NO MÍNIMO 4 (QUATRO) MEMBROS EM UM ÚNICO CLUSTER NO MODO ATIVO/ATIVO OU ATIVO/STAND-BY, OU SEJA, SENDO POSSÍVEL A DIVISÃO DE CARGAS ENTRE TODOS OS APPLIANCES, PERMITINDO O INVESTIMENTO GRADUAL AO LONGO DO TEMPO;
4.1.2.2 A SOLUÇÃO DEVE PERMITIR O AGRUPAMENTO DE MÚLTIPLOS EQUIPAMENTOS (CLUSTER) QUE FUNCIONEM COMO UM ÚNICO EQUIPAMENTO, COMPARTILHANDO ÚNICA CONFIGURAÇÃO DE POLÍTICA DE SEGURANÇA ENTRE OS COMPONENTES;
4.1.2.3 DEVE GARANTIR QUE TODAS AS CONFIGURAÇÕES SEJAM REPLICADAS ENTRE OS COMPONENTES DO CLUSTER, GARANTINDO A CONTINUIDADE DAS CONEXÕES MESMO SE UM DOS EQUIPAMENTOS DO CLUSTER ESTIVER INDISPONÍVEL;
4.1.2.4 DEVE POSSUIR MECANISMOS DE TESTE DE LINK COM O OBJETIVO DE FAZER COM QUE APPLIANCES DO CLUSTER FIQUEM OFFLINE SE HOUVER FALHA DE LINK ASSOCIADO AQUELE APPLIANCE;

4.1.3 DA DETECÇÃO DE ATAQUES.

4.1.3.1 A SOLUÇÃO DEVERÁ SUPORTAR ANÁLISE E DECODIFICAÇÃO DOS PROTOCOLOS DE REDE DE CAMADA 2 ATÉ A CAMADA 7 DO MODELO OSI (OPEN SYSTEM INTERCONNECTION);
4.1.3.2 A SOLUÇÃO OFERTADA DEVERÁ SER CAPAZ DE DECODIFICAR E ANALISAR, NO MÍNIMO, 150 (CENTO E

REQUISIÇÃO DE MATERIAL - RM - COM PRESTAÇÃO DE SERVIÇO
No.: 20200007 DATA DA RM: 07/01/2020

N.º COLETA: CP-20200015
LISTAGEM No.: 13324

PROGRAMA(S) DE TRABALHO: 03610206101411648

ORGÃO FISCAL: 8616 - DGTEC - DIVISAO DE REDES

PROCESSO: 2020617549
TIPO: VALOR TOTAL

OBJETO: SENSORES DE PREVENÇÃO DE INTRUSÃO (IPS)

PROCEDIMENTO ADOTADO: LICITAÇÃO

ITEM	CÓD. MATERIAL	NOME DO MATERIAL	UF	QTDE	PREÇO	VALOR

CINQUENTA) PROTOCOLOS, ENTRE OS QUAIS DEVERÃO CONSTAR: BOOTP, DHCP, DNS, HTTP, HTTPS, FTP, FINGER, ICMP VERSÃO 4, ICMP VERSÃO 6, IMAP, H323, IP VERSÃO 4, IP VERSÃO 6, LDAP, NETBIOS, POP3, NFS, RADIUS, SNMP, SMTP, SSH, SSL, TLS, RPC, TELNET, TCP, UDP, FTP E TFTP;
4.1.3.3 A SOLUÇÃO DEVE RECONHECER PELO MENOS OS SEGUINTES PROTOCOLOS: ETHERNET, H.323, GRE, IPV4, IPV6, ICMP, IPV4 ENCAPSULATION, IPV6 ENCAPSULATION, UDP, TCP, DNS, FTP, HTTP, HTTPS,IMAP, IMAPS, MGCP, MSRPC, NETBIOS DATAGRAM, OPC UA BINARY, OPC UA, ORACLE, MYSQL, POP3, POP3S, SIP, SRP, SSH, TELNET, WINS, X11, RTSP, SMTP, SUNRPC, NNTP, SCCP, SMB, SMB2 E TFTP;
4.1.3.4 A SOLUÇÃO DEVE SER CAPAZ DE IDENTIFICAR ATAQUES PARA OS PROTOCOLOS DE REDE INDEPENDENTEMENTE DAS PORTAS A QUE ESTEJAM RELACIONADOS, PARA NO MÍNIMO OS PROTOCOLOS FTP, HTTP´, HTTPS, POP3, SMTP, IMAP DNS, SNMP E RPC;
4.1.3.5 DEVE SER CAPAZ DE REALIZAR ANÁLISE E INSPEÇÃO STATEFULL (MANTENDO-SE O ESTADO DA CONEXÃO) E ANÁLISE E INSPEÇÃO STATELESS;
4.1.3.6 DEVE SUPORTAR ANALISE DE TRÁFEGO NA DIREÇÃO SERVIDOR-CLIENTE, OU SEJA, ATAQUES ORIGINADOS NO AMBIENTE EXTERNO E DIRECIONADOS A USUÁRIOS INTERNOS (CLIENT-SIDE ATTACKS OU DRIVE-BY ATTACKS);
4.1.3.7 DEVE SER CAPAZ DE DETECTAR BLOQUEIO DE ATAQUES DIRECIONADOS A SERVIDORES DE APLICAÇÃO WEB (WEB APPLICATION), ATRAVÉS DE TECNOLOGIA HEURÍSTICA OU ASSINATURAS PRÓPRIAS PARA A PROTEÇÃO CONTRA ESTE TIPO DE ATAQUE EM, NO MÍNIMO SQL-INJECTION E BUFFER OVERFLOW;
4.1.3.8 DEVE SER CAPAZ DE OBTER INFORMAÇÕES DETALHADAS SOBRE ATAQUES PARA LOCALIZAÇÃO GEOGRÁFICA, REPUTAÇÃO DE APLICAÇÃO E REPUTAÇÃO DE PROTOCOLO;
4.1.3.9 DEVE IMPLEMENTAR ALGORITMO DE PONTUAÇÃO PARA A RELEVÂNCIA DE UM ATAQUE CONFORME PADRÃO DE MERCADO E DEFINIDO POR ENTIDADE INDEPENDENTE (COMMON PLATFORM ENUMERATION), CVE ID OU BUGTRAQ ID, OU SUPORTAR MECANISMO PRÓPRIO DE PONTUAÇÃO DE ATAQUES, PERMITINDO DISTINGUIR QUANDO UM ATAQUE FOR PERMITIDO OU BLOQUEADO;
4.1.3.10 A SOLUÇÃO DEVE SUPORTAR A ANÁLISE DO NÍVEL DE RELEVÂNCIA DE UM ATAQUE, PERMITINDO UMA DEMONSTRAÇÃO DE FAIXA DE RELEVÂNCIA PARA, NO MÍNIMO, 4 (QUATRO) NÍVEIS;
4.1.3.11 DEVE SUPORTAR AS CATEGORIAS DE ATAQUES E TIPOS DE AMEAÇAS, CONFORME PADRÕES DE MERCADO E DEFINIDOS POR ENTIDADES INDEPENDENTES, PODENDO ESTAS SEREM IMPORTADAS EM PADRÃO SNORT;
4.1.3.12 DEVE SUPORTAR A CONFIGURAÇÃO E ADMINISTRAÇÃO PARA, NO MÍNIMO, OS SEGUINTES ITENS:
4.1.3.12.1 PERFIS DE DOS (DENIAL-OF-SERVICE) E DDOS (DISTRIBUTED DENIAL-OF-SERVICE);
4.1.3.12.2 REGRAS DE ACL (ACCESS CONTROL LIST);
4.1.3.12.3 CONTEXTOS DE ADMINISTRAÇÃO (VIRTUAL IPS) QUE DEVEM SER CONFIGURADOS POR VLAN (IEEE 802.1Q) E CIDR (CLASSLESS INTER-DOMAIN ROUTING);
4.1.3.13 DEVE SER CAPAZ DE DETECTAR E BLOQUEAR ATAQUES DO TIPO DENIAL-OF-SERVICE (DOS) E DISTRIBUTED DENIAL-OF-SERVICE (DDOS) DE FORMA NATIVA PARA:
4.1.3.13.1 DETECÇÃO E BLOQUEIO EFETIVO BASEADO EM ASSINATURAS DE ATAQUES ÀS VULNERABILIDADES DE DOS, CONFORME PADRÕES DE MERCADO E DEFINIDOS POR ENTIDADES INDEPENDENTES (COMPUTER EMERGENCY RESPONSE TEAM E COMMON VULNERABILITY AND EXPOSURES);
4.1.3.13.2 DETECÇÃO E BLOQUEIO EFETIVO BASEADO EM ASSINATURAS DE ATIVIDADES DE AGENTES ZUMBIS) DDOS, CONFORME PADRÕES DE MERCADO E DEFINIDOS POR ENTIDADES INDEPENDENTES (COMPUTER EMERGENCY RESPONSE TEAM E COMMON VULNERABILITY AND EXPOSURES);
4.1.3.13.3 DETECÇÃO E BLOQUEIO DE ATAQUE SYN, QUE PERMITA LIMITAR E CONTROLAR A QUANTIDADE DE REQUISIÇÕES DE CONEXÕES;
4.1.3.14 DEVE IMPLEMENTAR A DETECÇÃO E BLOQUEIO BASEADOS EM POLÍTICAS, PARA NO MÍNIMO:
4.1.3.14.1 FILTROS DE ORIGEM E DESTINO POR: PAÍS, NOME (DNS), ENDEREÇO IP, PORTA, BLOCO DE ENDEREÇOS, SISTEMAS AUTÔNOMOS, REDE OU GRUPO DE REDES;
4.1.3.14.2 VLAN ID PARA, NO MÍNIMO, 1024 VLANS;
4.1.3.14.3 FILTROS DE CONTROLE DE APLICAÇÃO: APLICAÇÃO, GRUPO DE APLICAÇÕES, PORTA DE COMUNICAÇÃO CUSTOMIZADA, SERVIÇO OU GRUPO DE SERVIÇOS;
4.1.3.14.4 FILTRO DE RESPOSTA COM, NO MÍNIMO OS ITENS SEGUINTES:
4.1.3.14.4.1 BLOQUEIO (DROP);
4.1.3.14.4.2 NEGAÇÃO (DENY);
4.1.3.14.4.3 QUARENTENA (BLOQUEAR OU NEGAR UM IP POR TEMPO DETERMINADO APÓS ATINGIR A QUANTIDADE DE EVENTOS RELATIVOS A UMA REGRA);
4.1.3.14.4.4 IGNORAR.
4.1.3.15 DEVE SER CAPAZ DE DETECTAR E BLOQUEAR O TRÁFEGO DE APLICAÇÕES INSTANT MESSENGER, P2P (PEER-TO-PEER) ALÉM DE PROXIES ANÔNIMOS;
4.1.3.16 DEVE SUPORTAR A DETECÇÃO E BLOQUEIO DE ATAQUES ATRAVÉS DE TUNEIS PARA IPV4-IN-IPV4, IPV4-IN-IPV6 E IPV6-IN-IPV6;
4.1.3.17 DEVE SUPORTAR A DETECÇÃO E BLOQUEIO DE ATAQUES ATRAVÉS DE VLANS.
4.1.3.18 A SOLUÇÃO DEVE SER TRANSPARENTE PARA, NO MÍNIMO OS SEGUINTES PROTOCOLOS: OSPF, BGP E VRRP OU SIMILAR.

REQUISIÇÃO DE MATERIAL - RM - COM PRESTAÇÃO DE SERVIÇO
No.: 20200007 DATA DA RM: 07/01/2020

N.º COLETA: CP-20200015
LISTAGEM No.: 13324

PROGRAMA(S) DE TRABALHO: 03610206101411648

ORGÃO FISCAL: 8616 - DGTEC - DIVISAO DE REDES

PROCESSO: 2020617549
TIPO: VALOR TOTAL

OBJETO: SENSORES DE PREVENÇÃO DE INTRUSÃO (IPS)

PROCEDIMENTO ADOTADO: LICITAÇÃO

ITEM	CÓD. MATERIAL	NOME DO MATERIAL	UF	QTDE	PREÇO	VALOR

4.1.3.19 A SOLUÇÃO DEVE SER CAPAZ DE NÃO INTERROMPER OU ALTERAR SEGMENTOS MONITORADOS COM PROTOCOLOS DE ROTEAMENTO E REDUNDÂNCIA DE ROTAS, AINDA QUE TRAFEGADOS DENTRO DO PROTOCOLO LACP (LINK AGGREGATION CONTROL PROTOCOL);
4.1.3.20 DEVE PERMITIR A CRIAÇÃO DE NOVAS ASSINATURAS DE ATAQUES;
4.1.3.21 DEVE PERMITIR A CONFIGURAÇÃO E ADMINISTRAÇÃO DE ACL EM CAMADA 3 COM AS SEGUINTES REGRAS:
4.1.3.21.1 PERMITIR: O TRÁFEGO É ENVIADO INLINE SEM INSPEÇÃO COMPLETA DOS PACOTES;
4.1.3.21.2 PERMITIR E PREVENIR ATAQUES: O TRÁFEGO É ENVIADO INLINE PARA INSPEÇÃO COMPLETA DOS PACOTES;
4.1.3.21.3 DESCARTAR: O TRÁFEGO SERÁ DESCARTADO;
4.1.3.22 DEVE SUPORTAR A DETECÇÃO DE BLOQUEIO DE ATAQUES, PELO MENOS, NAS SEGUINTES MODALIDADES:
4.1.3.22.1 INSPEÇÃO DE TRÁFEGO STATEFUL: IP DEFRAGMENTATION E TCP STREAM REASSEMBLY;
4.1.3.22.2 POR ASSINATURAS: DEFINIDAS PELO FABRICANTE E DEFINIDAS PELO USUÁRIO;
4.1.3.22.3 ANOMALIAS;
4.1.3.22.4 POR PROTOCOLOS DE CAMADA 7 DO MODELO OSI;
4.1.3.23 DEVE TER DETECÇÃO E BLOQUEIO DE ATAQUES, INDEPENDENTE DO SISTEMA OPERACIONAL ALVO;
4.1.3.24 DEVE SUPORTAR A DETECÇÃO HEURÍSTICA E CONSULTA DE REPUTAÇÃO DE ATIVIDADES DE AGENTES (ZUMBIS) INTERNOS QUE PERTENÇAM A UMA BOTNET;
4.1.3.25 DEVE SER CAPAZ DE IMPLEMENTAR O BLOQUEIO DE TRAFEGO PARA, NO MÍNIMO:
4.1.3.25.1 DIREÇÃO: INBOUND E OUTBOUND;
4.1.3.25.2 TIPO DE REGRA: BASEADA EM PROTOCOLO, PORTA E SERVIÇO;
4.1.3.26 A SOLUÇÃO DEVE SUPORTAR, NO MÍNIMO AS SEGUINTES CATEGORIAS E TIPOS DE ATAQUES:
4.1.3.26.1 RECONNAISSANCE: BRUTE FORCE, HOST SWEEP, OS FINGERPRINTING E PORT SCAN;
4.1.3.26.2 EXPLOITS: ARBITRARY COMMAND EXECUTION, BACKDOOR, BOT, BUFFER OVERFLOW, DENIAL OF SERVICE, DDOS AGENT ACTIVITY, CODE/SCRIPT EXECUTION, EVASION ATEMPT, PRIVILEGED ACCESS, PROBE, REMOTE ACCESS, TROJAN, VIRUS E WORMS;
4.1.3.26.3 VOLUME DOS: STATISTICAL DEVIATION E OVER THRESHOLD OU POSSUIR MECANISMO QUE PERMITA DETECÇÃO E CONTENÇÃO DE ATAQUES DOS;
4.1.3.26.4 POLICY VIOLATIONS: AUDIT, COMMAND SHELL, COVERT CHANNEL E NON-STANDARD PORT;
4.1.3.27 SUPORTAR ASSINATURAS PARA DETECÇÃO E BLOQUEIO DE ATAQUES ATRAVÉS DE VULNERABILIDADES DOS E DDOS;
4.1.3.28 DEVE SUPORTAR ASSINATURAS PARA DETECÇÃO E BLOQUEIO DE ATIVIDADES DE AGENTES (ZUMBIS) DDOS;
4.1.3.29 DEVE SUPORTAR APLICAÇÃO E REMOÇÃO DE QUARENTENA:
4.1.3.29.1 SOB DEMANDA DO ADMINISTRADOR, O QUAL DEVERÁ TER A OPÇÃO DE INSERIR E REMOVER UM ENDEREÇO IP DA QUARENTENA ATRAVÉS DE INTERFACE ADMINISTRATIVA SEM A NECESSIDADE DE REINICIALIZAÇÃO DO EQUIPAMENTO OU REAPLICAÇÃO DE POLÍTICA;
4.1.3.29.2 POR PERÍODOS PROGRAMÁVEIS PELO ADMINISTRADOR, PODENDO SER ESSES (OS PERÍODOS) DIFERENTES EM CADA REGRA;
4.1.3.29.3 POR REMOÇÃO EXPLICITA, APÓS EXPIRAÇÃO DE TEMPO PRÉ-DETERMINADO;
4.1.3.30 A SOLUÇÃO DEVE SUPORTAR AJUSTE DE BLOQUEIO INTELIGENTE, BASEADO EM ASSINATURAS RECOMENDADAS PELO FABRICANTE PARA BLOQUEIO;
4.1.3.31 DEVERÁ PERMITIR A VISUALIZAÇÃO DE BLOQUEIOS DE PACOTES E DE CONEXÕES, INDEPENDENTE DO MOTIVO PELOS QUAIS OCORRERAM.

4.1.4 DA DETECÇÃO DE AMEAÇAS (MALWARES)

4.1.4.1 A SOLUÇÃO DEVE REALIZAR A DETECÇÃO E BLOQUEIO DE CÓDIGOS MALICIOSOS, AMEAÇAS MALWARES E MALWARES AVANÇADOS EM TEMPO REAL, UTILIZANDO-SE OS SEGUINTES MECANISMOS:
4.1.4.1.1 MECANISMO DE LISTA LOCAL DE ARQUIVOS CONFIÁVEIS (LISTA BRANCA), OS QUAIS NÃO PRECISARÃO SER ANALISADOS POR SEREM CONFIÁVEIS;
4.1.4.1.2 MECANISMO DE LISTA COM VALORES HASH DE ARQUIVOS QUE SEJAM CÓDIGOS MALICIOSOS E AMEAÇAS (MALWARES) CONHECIDAS E ARMAZENADO EM UMA BASE DE DADOS LOCAL (LISTA NEGRA);
4.1.4.1.3 MECANISMOS DE DETECÇÃO DE CÓDIGOS MALICIOSOS E AMEAÇAS (MALWARES), QUE DEVE OPERAR EM TEMPO REAL, PARA NO MÍNIMO OS SEGUINTES ITENS:
4.1.4.1.3.1 ARQUIVOS PDF;
4.1.4.1.3.2 OBJETOS E ARQUIVOS FLASH;
4.1.4.1.3.3 ARQUIVOS EXECUTÁVEIS;
4.1.4.1.3.4 ARQUIVOS MICROSOFT OFFICE.

REQUISIÇÃO DE MATERIAL - RM - COM PRESTAÇÃO DE SERVIÇO
No.: 20200007 DATA DA RM: 07/01/2020

N.º COLETA: CP-20200015
LISTAGEM No.: 13324

PROGRAMA(S) DE TRABALHO: 03610206101411648

ORGÃO FISCAL: 8616 - DGTEC - DIVISAO DE REDES

PROCESSO: 2020617549
TIPO: VALOR TOTAL

OBJETO: SENSORES DE PREVENÇÃO DE INTRUSÃO (IPS)

PROCEDIMENTO ADOTADO: LICITAÇÃO

ITEM	CÓD. MATERIAL	NOME DO MATERIAL	UF	QTDE	PREÇO	VALOR

4.1.5 DA RESPOSTA AOS ATAQUES.

4.1.5.1 A SOLUÇÃO DEVE SUPORTAR TCP RESET1
4.1.5.2 DEVE IMPLEMENTAR O BLOQUEIO DE PACOTES;
4.1.5.3 DEVE IMPLEMENTAR A ATUALIZAÇÃO GLOBAL DE BLOQUEIO PARA DETERMINADO ATAQUE DE MODO A PROPAGAR E ATUALIZAR TODAS AS POLÍTICAS;
4.1.5.4 DEVE SUPORTAR A CAPTURA DE PACOTES PARA ANÁLISE DE EVIDÊNCIAS EM FORMATO LIBPCAP (LIBRARY FOR PACKET CAPTURE);
4.1.5.5 DEVE SUPORTAR O ENVIO DE TRAP SNMP PARA SNMPV2 E SNMPV3;
4.1.5.6 DEVE IMPLEMENTAR O ENVIO DE EMAIL;

4.1.6 DAS INTERFACES DE INSPEÇÃO;

4.1.6.1 A SOLUÇÃO DEVERÁ FORNECER DOIS EQUIPAMENTOS COM, NO MÍNIMO 8 INTERFACES UTP E 8 INTERFACES SFP CADA UM;
4.1.6.2 CADA INTERFACE, DE CADA EQUIPAMENTO, DEVERÁ FORNECER NO MÍNIMO 10 GBPS DE THROUGHPUT;
4.1.6.3 CADA EQUIPAMENTO DEVERÁ POSSUIR NO MÍNIMO UMA INTERFACE DE GERÊNCIA UTP.
4.1.6.4 PARA CADA INTERFACE DO TIPO SFP DEVERÁ SER FORNECIDO O RESPECTIVO TRANSCEIVER MULTIMODO PARA CONEXÃO;
4.1.6.5 AS INTERFACES DEVEM PERMITIR INDIVIDUALMENTE AS SEGUINTES CONFIGURAÇÕES EM CASO DE FALHAS:
4.1.6.5.1 DISPONIBILIDADE (FAIL-OPEN) DOS SEGMENTOS MONITORADOS ATRAVÉS DE DISPOSITIVO INTERNO OU EXTERNO DE BYPASS;
4.1.6.5.2 INDISPONIBILIDADE (FAIL-CLOSE) DOS SEGMENTOS MONITORADOS;
4.1.6.5.3 TODAS AS INTERFACES COM EXCEÇÃO DA INTERFACE DE GERÊNCIA, DEVEM POSSUIR A FUNCIONALIDADE DE BYPASS;
4.1.6.5.4 A SOLUÇÃO DEVE SER CAPAZ, POR CONFIGURAÇÃO DO ADMINISTRADOR, DE DESATIVAR AUTOMATICAMENTE UMA INTERFACE, CASO DETECTE QUEDA DE LINK NA OUTRA INTERFACE DO MESMO SEGUIMENTO DE REDE;
4.1.6.5.5 A SOLUÇÃO DEVE SUPORTAR CONFIGURAÇÃO FLEXÍVEL DE PASS-THROUGH EM CAMADA 2 PARA TRÁFEGO QUE ULTRAPASSE A ANÁLISE DE TRÁFEGO AGREGADO SUPORTADO PELA SOLUÇÃO DE NIPS;

4.1.7 DO DESEMPENHO E DA ESCALABILIDADE;

4.1.7.1 A SOLUÇÃO PODE INSERIR LATÊNCIA DE, NO MÁXIMO, 150 µS (CENTO E CINQUENTA MICROSSEGUNDOS) PARA TRÁFEGO CRIPTOGRAFADO NOS SEGMENTOS DE REDE MONITORADOS, COM EXCEÇÃO NOS CASOS ONDE HOUVER NECESSIDADE DE CONSULTA EXTERNA TAIS COMO CONSULTA DNS.
4.1.7.2 A SOLUÇÃO DEVE MONITORAR E PROTEGER OS SEGMENTOS DE REDE MONITORADOS EM MODO TRANSPARENTE, ASSIM COMO OPERAR NA CAMADA 2 DO MODELO OSI, OU SEJA, A INTERFACE DE MONITORAÇÃO NÃO DEVE REQUERER ENDEREÇOS IP E ENDEREÇOS MAC;
4.1.7.3 DEVE SUPORTAR, DE FORMA HOMOGÊNEA E HETEROGÊNEA, OS SEGUINTES MODOS DE OPERAÇÃO:
4.1.7.3.1 PREVENÇÃO (IN-LINE) - MONITORAÇÃO E PROTEÇÃO DE SEGMENTOS DE REDE EM AMBAS AS DIREÇÕES, PERMITINDO MONITORAR E RESPONDER À ATAQUES EM TEMPO REAL, MANTENDO-SE O ESTADO DAS CONEXÕES (STATEFUL);
4.1.7.3.2 BLOQUEIO SIMULADO (IN-LINE) - MONITORAÇÃO E SIMULAÇÃO DE PROTEÇÃO DE SEGMENTOS DE REDE EM AMBAS AS DIREÇÕES, PERMITINDO MONITORAR E ALERTAR OS ATAQUES EM TEMPO REAL, REPORTANDO QUAIS ATAQUES SERIAM BLOQUEADOS, MANTENDO-SE O ESTADO DAS CONEXÕES (STATEFUL);
4.1.7.3.3 MONITORAÇÃO (SPAN) - MONITORAÇÃO DE SEGMENTOS DE REDE, PERMITINDO MONITORAR E ALERTAR OS ATAQUES EM TEMPO REAL;
4.1.7.4 DEVE PERMITIR A CAPTURA DE TODOS OS PACOTES PARA FINALIDADE DE TROUBLESHOOTING EM FORMATO LIBPCAP (LIBRARY FOR PACKET CAPTURE), PODENDO SER ATRAVÉS DE FERRAMENTA ESPECÍFICA OU ATRAVÉS DE INTERFACE GRÁFICA QUE PERMITA REGRAS DE CAPTURA, SEM AFETAR A DISPONIBILIDADE E DESEMPENHO DOS SEGMENTOS DE REDE;
4.1.7.5 DEVE PERMITIR INSTALAÇÃO SEM NECESSIDADE DE RECONFIGURAÇÃO DE ROTEADORES E SWITCHES, QUANDO NO MODO DE OPERAÇÃO IN-LINE.

4.1.8 DA CAPACIDADE MÍNIMA DE OPERAÇÃO.

4.1.8.1 A SOLUÇÃO DEVE SUPORTAR UM TRÁFEGO TOTAL DE 40 GBPS E UM TOTAL DE ANÁLISE E INSPEÇÃO DE

ITEM	CÓD. MATERIAL	NOME DO MATERIAL	UF	QTDE	PREÇO	VALOR

TRAFEGO NGIPS DE 20 GBPS.
4.1.8.2 O TRÁFEGO (TOTAL DE INSPEÇÃO) DEVEM SER MEDIDOS EM PADRÃO IMIX (INTERNET MIX)
4.1.8.3 A SOLUÇÃO DEVE SUPORTAR A ANÁLISE E INSPEÇÃO DE, NO MÍNIMO, 2 GBPS DE TRÁFEGO SSL POR CAIXA, TOTALIZANDO 4GBPS.
4.1.8.4 DEVE SUPORTAR NO MÍNIMO 10.000.000 (DEZ MILHÕES) DE CONEXÕES CONCORRENTES E UMA TAXA DE, NO MÍNIMO, 300.000 NOVAS CONEXÕES TCP POR SEGUNDO;
4.1.8.5 A SOLUÇÃO DEVE FAZER A INSPEÇÃO DE TODA SESSÃO, INDEPENDENTEMENTE DO TAMANHO, SEM DEGRADAR A PERFORMANCE DO EQUIPAMENTO;
4.1.8.6 A SOLUÇÃO DE IPS DEVE FAZER A INSPEÇÃO DE TODO O TRAFEGO DE FORMA BIDIRECIONAL, ANALISANDO QUALQUER TAMANHO DE SESSÃO SEM DEGRADAR A PERFORMANCE DO EQUIPAMENTO;
4.1.8.7 NÃO SERÃO ACEITAS SOLUÇÕES QUE POSSUAM MECANISMO PARA INSPECIONAR SOMENTE UMA PARTE DA SESSÃO;

4.1.9 DAS DEMAIS CARACTERÍSTICAS DA SOLUÇÃO.

4.1.9.1 A SOLUÇÃO DEVE SER CAPAZ DE SER MONTADA EM RACK (BASTIDOR) DE 19 POLEGADAS;
4.1.9.2 A SOLUÇÃO DEVE SUPORTAR, NO MÍNIMO, 2 (DUAS) FONTES DE ENERGIA INTERNAS, PARA CORRENTE ALTERNADA (AC - ALTERNATING CURRENT), COM CHAVEAMENTO AUTOMÁTICO E CAPACIDADE DE OPERAÇÃO EM 100V A 240V (50 E 60HZ), CONFORME INFORMADO ABAIXO:
4.1.9.2.1 AS FONTES DE ENERGIA DEVEM SER DO TIPO SUBSTITUÍVEL (HOT-SWAP), PERMITINDO INSTALAÇÃO E/OU SUBSTITUIÇÃO SEM A NECESSIDADE DE REMOÇÃO DO EQUIPAMENTO;
4.1.9.2.2 AS FONTES DE ENERGIA DEVEM SER SUFICIENTES PARA MANTER TODAS AS OPERAÇÕES DA SOLUÇÃO, MESMO NO CASO DE FALHA DE UMA DAS FONTES DE ENERGIA, INDEPENDENTEMENTE DA QUANTIDADE DE INTERFACES EM USO OU FUNCIONALIDADES HABILITADAS;
4.1.9.2.3 AS FONTES DE ENERGIA DEVEM VIR ACOMPANHADAS COM CABOS DE ENERGIA COM NO MÍNIMO 1,80 M (UM METRO E OITENTA CENTÍMETROS) DE COMPRIMENTO;
4.1.9.3 DEVE SUPORTAR UMA FAIXA DE 10% A 85% DE UMIDADE RELATIVA E 10 °C A 35 °C TEMPERATURA AMBIENTE, SEM CONDENSAÇÃO;
4.1.9.4 DEVE POSSUIR UNIDADES DE VENTILAÇÃO REDUNDANTES, PODE SER DO TIPO SUBSTITUÍVEL (HOTSWAP), PERMITINDO QUE FLUXO DE AR (EXAUSTÃO) OCORRA EM DIREÇÃO A PARTE TRASEIRA DO RACK;
4.1.9.5 DEVE POSSUIR AS INTERFACES DE MONITORAÇÃO LOCALIZADAS NA PARTE FRONTAL;
4.1.9.6 DEVE POSSUIR INTERFACE SERIAL RS-232 OU INTERFACE USB OU INTERFACE RJ45 EXCLUSIVA E DEDICADA PARA ACESSO À CONSOLE DO EQUIPAMENTO, SENDO NECESSÁRIO O FORNECIMENTO DO RESPECTIVO CABO COMPATÍVEL;
4.1.9.7 DEVE PERMITIR ACESSO REMOTO, ATRAVÉS DE SSH, À CONSOLE DO EQUIPAMENTO;
4.1.9.8 DEVE SER FORNECIDA COM TODOS OS RESPECTIVOS CABEAMENTOS, TRANSMISSORES-RECEPTORES E CONECTORES NECESSÁRIOS PARA OPERAÇÃO DAS INTERFACES DE MONITORAÇÃO E CONEXÃO COM O AMBIENTE;
4.1.9.8.1 O CABEAMENTO DEVE DEVERÁ TER PELO MENOS 3 (TRÊS) METROS E SER FORNECIDO JÁ CONECTORIZADO E TESTADO;
4.1.9.8.2 OS MÓDULOS DE INTERFACES QUE NECESSITEM DE SEUS RESPECTIVOS TRANSMISSORES-RECEPTORES DEVEM SER FORNECIDOS INTEGRALMENTE, ISTO É, CASO OS MÓDULOS DE INTERFACES DO EQUIPAMENTO EXCEDAM AS QUANTIDADES MÍNIMAS REQUERIDAS, AINDA ASSIM DEVEM SER FORNECIDOS OS SEUS RESPECTIVOS TRANSMISSORES-RECEPTORES;
4.1.9.8.3 A CONTRATADA DEVERÁ FORNECER TODO O CABEAMENTO NECESSÁRIO PARA A INTERLIGAÇÃO DOS EQUIPAMENTOS, TANTO QUANTO FOREM AS INTERFACES DISPONÍVEIS.
4.1.9.8.4 PARA INTERFACE 1000BASE-T DEVE SER ADOTADO CABEAMENTO CAT6A E PARA INTERFACE 10GBASE-SR DEVE SER ADOTADO CABEAMENTO COMPOSTO POR FIBRAS MULTI-MODO OM3 DE DIÂMETRO 50 µM/125 µM;
4.1.9.9 O FUNCIONAMENTO DO BYPASS (FAIL-OPEN) NÃO DEVE AFETAR O TRÁFEGO DE REDE EM CASO DE FALHA DAS INTERFACES;
4.1.9.10 O FUNCIONAMENTO DO BYPASS (FAIL-OPEN) NÃO DEVE AFETAR O TRÁFEGO DE REDE EM CASO DE FALHA DO EQUIPAMENTO;
4.1.9.11 A SOLUÇÃO DEVE POSSUIR CONFIGURAÇÕES DE CPU E MEMÓRIA (RAM E FLASH) SUFICIENTES PARA A IMPLEMENTAÇÃO DE TODAS AS FUNCIONALIDADES DESCRITAS NESTE TERMO DE REFERÊNCIA;
4.1.9.12 DEVE POSSUIR ARMAZENAMENTO DO TIPO SSD (SOLID STATE DISK);
4.1.9.13 CASO A SOLUÇÃO POSSUA AS DUAS TECNOLOGIAS DE DISCO SIMULTÂNEOS NO MESMO EQUIPAMENTO, SERÃO ACEITOS DISCOS DO TIPO HDD(HARD DISK DRIVE), DESDE QUE O SISTEMA OPERACIONAL DO EQUIPAMENTO SEJA INSTALADO NOS DISCOS DO TIPO SSD(SOLID STATE DISK).

4.1.10 O GERENCIAMENTO DA SOLUÇÃO.

REQUISIÇÃO DE MATERIAL - RM - COM PRESTAÇÃO DE SERVIÇO
No.: 20200007 DATA DA RM: 07/01/2020

N.º COLETA: CP-20200015
LISTAGEM No.: 13324

PROGRAMA(S) DE TRABALHO: 03610206101411648

ORGÃO FISCAL: 8616 - DGTEC - DIVISAO DE REDES

PROCESSO: 2020617549
TIPO: VALOR TOTAL

OBJETO: SENSORES DE PREVENÇÃO DE INTRUSÃO (IPS)

PROCEDIMENTO ADOTADO: LICITAÇÃO

ITEM	CÓD. MATERIAL	NOME DO MATERIAL	UF	QTDE	PREÇO	VALOR

4.1.10.1 SOLUÇÃO DEVE PERMITIR O GERENCIAMENTO POR DASHBOARD CENTRALIZADO;
4.1.10.2 DEVERÁ SER FORNECIDO DASHBOARD PARA A FUNCIONALIDADE ÚNICA E EXCLUSIVA DE GERENCIAMENTO DA SOLUÇÃO.
4.1.10.3 O DASHBOARD DE GERENCIAMENTO DEVE POSSUIR AS POLÍTICAS BASEADAS EM ASSINATURAS RECOMENDADAS PELO FABRICANTE PARA BLOQUEIO, CONFORME RECOMENDAÇÕES DE SUA EQUIPE TÉCNICA;
4.1.10.4 DASHBOARD DE GERENCIAMENTO DEVE SUPORTAR A ATUALIZAÇÃO DE SOFTWARE E FIRMWARE DA SOLUÇÃO DE IPS, DE FORMA REMOTA E CENTRALIZADA NOS SEGUINTES MODOS:
4.1.10.4.1 ONLINE: AUTOMÁTICA E MANUAL DE CONTEÚDO DE SEGURANÇA E PRODUTO ATRAVÉS DA INTERNET, PODENDO SER REALIZADA SEM INTERFERÊNCIA DO USUÁRIO;
4.1.10.4.2 OFFLINE: AUTOMÁTICA E MANUAL DE CONTEÚDO DE SEGURANÇA E PRODUTO ATRAVÉS DE PACOTES DE ATUALIZAÇÃO IMPORTADOS PELA GERÊNCIA, SEM CONEXÃO COM A INTERNET;
4.1.10.5 DASHBOARD DE GERENCIAMENTO DEVE SUPORTAR A APLICAÇÃO E REVOGAÇÃO DE POLÍTICAS E REGRAS DE FORMA CENTRALIZADA, SEM AFETAR A DETECÇÃO E BLOQUEIO;
4.1.10.6 DEVE PERMITIR O ENVIO DE REGISTROS DE EVENTOS ATRAVÉS DE INTEGRAÇÃO COM SERVIDOR DE LOG;
4.1.10.7 DASHBOARD DE GERENCIAMENTO DEVE SUPORTAR INTEGRAÇÃO, ATRAVÉS DE SNMPV2 E SNMPV3 E FORNECER OS RESPECTIVOS ARQUIVOS DE MIBS;
4.1.10.8 O DASHBOARD DE GERENCIAMENTO DEVE PERMITIR SINCRONISMO DE HORÁRIO DA SOLUÇÃO ATRAVÉS DE INTEGRAÇÃO COM SERVIDOR NTP (NETWORK TIME PROTOCOL);
4.1.10.9 DEVE SUPORTAR OPERAÇÃO E ARMAZENAMENTO COM CAPACIDADE DE 20.000.000 (VINTE MILHÕES) DE EVENTOS, NA PRÓPRIA GERÊNCIA OU SERVIDOR EXTERNO, COM SISTEMA GERENCIADOR DE BANCO DE DADOS RELACIONAL (SGBDR - RELATIONAL DATABASE MANAGEMENT SYSTEM OU RDBMS) QUE UTILIZE LINGUAGEM DE PESQUISA DECLARATIVA SQL (STRUCTURED QUERY LANGUAGE), OU UTILIZAR CONSOLE DE LOGS DO PRÓPRIO FABRICANTE PARA ANÁLISE DE EVENTOS, SENDO POSSÍVEL O ENVIO LOGS PARA SYSLOG EXTERNO;
4.1.10.10 DEVE PERMITIR O ARQUIVAMENTO (BACKUP) DOS EVENTOS GERADOS PELA SOLUÇÃO DE NIPS, CONFORME SE SEGUE:
4.1.10.10.1 MANUAL: ARQUIVAMENTO (BACKUP) DOS EVENTOS SOB DEMANDA;
4.1.10.10.2 AUTOMÁTICO: ARQUIVAMENTO (BACKUP) DOS EVENTOS DE FORMA AGENDADA E AUTOMÁTICA.
4.1.10.11 O GERENCIAMENTO DEVE PERMITIR O BACKUP E O RESTORE DE SUA BASE DE DADOS;
4.1.10.12 DEVE PERMITIR A CONFIGURAÇÃO E ADMINISTRAÇÃO DE CONTAS DE ACESSO DE USUÁRIOS E ADMINISTRADORES ATRAVÉS DE AUTENTICAÇÃO LOCAL OU VIA SERVIÇO DE DIRETÓRIO.
4.1.10.13 O DASHBOARD DE GERENCIAMENTO DEVE SUPORTAR A ATRIBUIÇÃO DE, NO MÍNIMO, OS PERFIS DE USUÁRIO (SOMENTE LEITURA), ADMINISTRADOR (LEITURA E ESCRITA) E SUPERUSUÁRIO;
4.1.10.14 DEVE PERMITIR A MONITORAÇÃO DE, NO MÍNIMO, OS SEGUINTES RECURSOS DA SOLUÇÃO DE IPS:
4.1.10.14.1 TAXA DE TRANSFERÊNCIA DAS INTERFACES DOS EQUIPAMENTOS;
4.1.10.14.2 TAXA DE TRANSFERÊNCIA DE TRÁFEGO INSPECIONADO;
4.1.10.14.3 PERCENTUAL DE UTILIZAÇÃO DE CPU;
4.1.10.14.4 PERCENTUAL DE UTILIZAÇÃO DE MEMÓRIA
4.1.10.14.5 QUANTIDADE DE CONEXÕES CORRENTES ESTABELECIDAS;
4.1.10.14.6 TAXA DE NOVAS CONEXÕES POR SEGUNDO.
4.1.10.15 O DASHBOARD DE GERENCIAMENTO DEVE SUPORTAR NOTIFICAÇÃO DE FALHAS DE SISTEMA, DE MODO A PERMITIR O ENVIO DE INFORMAÇÕES ATRAVÉS DE INTEGRAÇÃO COM SERVIDOR DE LOG OU COM SERVIDOR SNMP;
4.1.10.16 A APLICAÇÃO DEVE POSSUIR NATIVAMENTE A CAPACIDADE DE GERAÇÃO DE RELATÓRIOS DE FORMA MANUAL (SOB DEMANDA) E AUTOMÁTICA (PRÉ-AGENDADA);
4.1.10.17 O DASHBOARD DE GERENCIAMENTO DEVE PERMITIR A EXPORTAÇÃO DE RELATÓRIOS PARA ARQUIVOS HTML, CSV OU PDF;
4.1.10.18 O DASHBOARD DE GERENCIAMENTO DEVE POSSUIR RELATÓRIOS PRÉ-DEFINIDOS, NO MÍNIMO PARA:
4.1.10.18.1 RESUMO EXECUTIVO;
4.1.10.18.2 ATAQUES DE RECONHECIMENTO;
4.1.10.18.3 ANÁLISE DE TENDÊNCIAS;
4.1.10.18.4 OS 10 (DEZ) ATAQUES MAIS DETECTADOS;
4.1.10.18.5 AS 10 (DEZ) AMEAÇAS (MALWARES) MAIS DETECTADAS;
4.1.10.18.6 AS 10 (DEZ) ORIGENS QUE MAIS ATACARAM;
4.1.10.18.7 OS 10 (DEZ) DESTINOS QUE MAIS FORAM ATACADOS;
4.1.10.19 PERMITIR CUSTOMIZAÇÃO E CRIAÇÃO DE RELATÓRIOS SOB DEMANDA, PERMITINDO UTILIZAÇÃO DE FILTROS ESPECÍFICOS, NO MÍNIMO PARA:
4.1.10.19.1 ENDEREÇO IP DE ORIGEM;
4.1.10.19.2 ENDEREÇO IP DE DESTINO;
4.1.10.19.3 PAÍS DE ORIGEM;
4.1.10.19.4 PAÍS DE DESTINO;
4.1.10.19.5 IDENTIFICAÇÃO DO USUÁRIO DE ORIGEM;
4.1.10.19.6 IDENTIFICAÇÃO DO USUÁRIO DE DESTINO;
4.1.10.19.7 NOME DO ATAQUE;

REQUISIÇÃO DE MATERIAL - RM - COM PRESTAÇÃO DE SERVIÇO
No.: 20200007 DATA DA RM: 07/01/2020

N.º COLETA: CP-20200015
LISTAGEM No.: 13324

PROGRAMA(S) DE TRABALHO: 03610206101411648

ORGÃO FISCAL: 8616 - DGTEC - DIVISAO DE REDES

PROCESSO: 2020617549
TIPO: VALOR TOTAL

OBJETO: SENSORES DE PREVENÇÃO DE INTRUSÃO (IPS)

PROCEDIMENTO ADOTADO: LICITAÇÃO

ITEM	CÓD. MATERIAL	NOME DO MATERIAL	UF	QTDE	PREÇO	VALOR
2						48.000,00
3						254.217,08
4						63.621,00
5						39.863,94
6						1.298.431,95

VALOR TOTAL DA RM DE COMPRA: R$ 2.315.312,67 (DOIS MILHÕES, TREZENTOS E QUINZE MIL, TREZENTOS E DOZE REAIS E SESSENTA E SETE CENTAVOS)
VALOR TOTAL DE SERVIÇO: R$ 1.704.133,97 (UM MILHÃO, SETECENTOS E QUATRO MIL, CENTO E TRINTA E TRÊS REAIS E NOVENTA E SETE CENTAVOS)
VALOR TOTAL DA RM: R$ 4.019.446,64 (QUATRO MILHÕES, DEZENOVE MIL, QUATROCENTOS E QUARENTA E SEIS REAIS E SESSENTA E QUATRO CENTAVOS)

DISTRIBUIÇÃO DE VALORES POR CÓDIGO DE DESPESA

CÓD. DESPESA	VALOR
44905239	R$2.315.312,67
33903900	R$ 1.704.133,97
TOTAL:	R$ 4.019.446,64

NOTAS:

OS COMPONENTES DA SOLUÇÃO E DEMAIS ACESSÓRIOS, BEM COMO O DASHBOARD DE GERÊNCIA DEVERÃO SER ENTREGUES EM ATÉ 45 (QUARENTA E CINCO) DIAS CORRIDOS, CONTADOS DA DATA DE PUBLICAÇÃO DO EXTRATO DO CONTRATO NO DIÁRIO DA JUSTIÇA ELETRÔNICO.

A ENTREGA DOS COMPONENTES DA SOLUÇÃO E DEMAIS ACESSÓRIOS DEVERÁ SER FEITA NAS DEPENDÊNCIAS DA DIVISÃO DE REDES DO DEPARTAMENTO DE INFRAESTURA DA DIRETORIA DE TECNOLOGIA DO PODER JUDICIÁRIO DO ESTADO DO RIO DE JANEIRO, SITUADA NA AVENIDA ERASMO BRAGA Nº - 115 - 1º ANDAR - CORREDOR C - SALA 111 - LÂMINA I, APÓS AGENDAMENTO COM ATÉ 48 (QUARENTA E OITO) HORAS DA DATA PREVISTA PARA ENTREGA, ATRAVÉS DO ENDEREÇO ELETRÔNICO DIRED.LICITA@TJRJ.JUS.BR OU ATRAVÉS DOS TELEFONES (21)3133-1813 OU (21)3133-3406 DA SECRETARIA DA DIVISÃO DE REDES.

A GARANTIA DE QUALIDADE DEVERÁ SER DA CONTRATADA, PELO PRAZO MÍNIMO DE 48 (QUARENTA E OITO) MESES, A CONTAR DA EMISSÃO DO MEMORANDO DE INÍCIO DA CONTRATAÇÃO.

AS DEMAIS INFORMAÇÕES ESTÃO CONSIGNADAS NO TERMO DE REFERÊNCIA.

INSTRUÇÃO ELABORADA EM CONFORMIDADE COM O ATO NORMATIVO Nº 03/19 DO PJERJ.

REQUISIÇÃO DE MATERIAL - RM - COM PRESTAÇÃO DE SERVIÇO
No.: 20200007 DATA DA RM: 07/01/2020

N.º COLETA: CP-20200015
LISTAGEM No.: 13324

PROGRAMA(S) DE TRABALHO: 03610206101411648

ORGÃO FISCAL: 8616 - DGTEC - DIVISAO DE REDES

PROCESSO: 2020617549
TIPO: VALOR TOTAL

OBJETO: SENSORES DE PREVENÇÃO DE INTRUSÃO (IPS)

PROCEDIMENTO ADOTADO: LICITAÇÃO

ITEM	CÓD. MATERIAL	NOME DO MATERIAL	UF	QTDE	PREÇO	VALOR

VALOR TOTAL DA RM DE COMPRA: R$ 2.315.312,67 (DOIS MILHÕES, TREZENTOS E QUINZE MIL, TREZENTOS E DOZE REAIS E SESSENTA E SETE CENTAVOS)
VALOR TOTAL DE SERVIÇO: R$ 1.704.133,97 (UM MILHÃO, SETECENTOS E QUATRO MIL, CENTO E TRINTA E TRÊS REAIS E NOVENTA E SETE CENTAVOS)
VALOR TOTAL DA RM: R$ 4.019.446,64 (QUATRO MILHÕES, DEZENOVE MIL, QUATROCENTOS E QUARENTA E SEIS REAIS E SESSENTA E QUATRO CENTAVOS)

CHEFE DO SERVIÇO DE INSTRUÇÃO DE COMPRAS DE MATERIAIS

MATRÍCULA:

DIRETOR DA DIVISÃO DE PLANEJAMENTO E INSTRUÇÃO DE COMPRAS DE MATERIAIS

MATRÍCULA:

DIRETOR DO DEPTO. PATR. E MATERIAL

MATRÍCULA: