ADENDO 01 AO PREGÃO ELETRÔNICO Nº 28/2024

A Comissão Permanente de Contratação do Tribunal de Justiça do Estado do Ceará comunica aos interessados que o Edital do **Pregão Eletrônico n.º 28/2024 – Processo nº 8510187-89.2024.8.06.0000**, que trata da **"Registro de preços para futura e eventual contratação de empresa especializada em tecnologia da informação para fornecimento de licenças de uma solução de segurança de Endpoint com funcionalidades de EDR/XDR, incluindo os serviços de instalação, configuração, implantação e treinamento da solução e demais especificações e características consignados, incluindo suporte e garantia pelo período de 60 meses"** sofreu as seguintes alterações na peça editalícia:

NO EDITAL:

Exclusão dos itens **3.4.1.1.14, 3.4.1.1.15, 3.4.1.1.19, 3.4.1.1.25, 3.4.1.1.34, 3.4.1.1.35, 3.4.1.1.36, 3.4.1.1.37, 3.4.1.1.38, 3.4.1.1.39, 3.4.1.1.41, 3.4.1.1.42, 3.4.1.1.68, 3.4.1.1.69, 3.4.1.1.70, 3.4.1.1.71, 3.4.1.1.72, 3.4.1.1.73, 3.4.1.1.74, 3.4.1.1.75, 3.4.1.1.76, 3.4.1.1.78, 3.4.1.1.79, 3.4.1.1.80, 3.4.1.1.82, 3.4.1.1.86, 3.4.1.1.94, 3.4.1.1.95, 3.4.1.1.100, 3.4.1.1.108, 3.4.2.3.1, 3.4.2.3.2, 3.4.2.3.3, 3.4.2.3.4, 3.4.2.4.9, 3.4.2.4.10, 3.4.2.4.11, 3.4.2.4.34, 3.4.2.4.26, 3.4.2.4.35, 3.4.3.1.1, 3.4.3.2.8, 3.4.3.2.9, 3.4.3.2.26, 3.4.4.3.18, 3.4.5.2.10, 3.4.6.2.9, 3.4.10.1, 3.4.10.2, 3.4.10.4, 3.4.10.5, 3.4.10.7, 3.4.10.13, 3.4.10.14, 3.4.10.17, 3.4.10.18, 3.4.10.19, 3.4.10.20, 3.4.10.21, 3.4.10.23, 3.4.10.25, 3.4.10.26, 3.4.10.28, 3.4.12.2.4.**

ONDE SE LÊ:

3.4.1.1.8. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;

LEIA-SE:

3.4.1.1.8. As licenças e proteção devem estar disponíveis durante toda a vigência do suporte e garantia;

ONDE SE LÊ:

3.4.1.1.11. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, através da console de gerenciamento e GPO de AD;

LEIA-SE:

3.4.1.1.11. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, por meio do GPO de AD;

ONDE SE LÊ:

3.4.1.1.22. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;

LEIA-SE:

3.4.1.1.22. Capacidade de instalar atualizações em grupos de computadores específicos antes de instalar nos demais computadores da rede;

ONDE SE LÊ:

3.4.1.1.24. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

LEIA-SE:

3.4.1.1.24. Capacidade de atualizar os pacotes de instalação com as últimas vacinas ou/e ter a capacidade de manter as funcionalidades e capacidades de detecção e prevenção sempre atualizadas através de uma conexão persistente com a arquitetura em nuvem do fornecedor;

ONDE SE LÊ:

3.4.1.1.27. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

LEIA-SE:

3.4.1.1.27. Capacidade de desinstalar ou bloquear remotamente qualquer software instalado nas máquinas clientes;

ONDE SE LÊ:

3.4.1.1.43. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

LEIA-SE:

3.4.1.1.43. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado, evidenciando na console de gerenciamento como o ativo foi descoberto, permitindo que a equipe responsável realize a instalação do agente da solução, caso a instalação não tenha sido feita de forma automática;

ONDE SE LÊ:

3.4.1.1.51. Minutos/horas desde a última atualização de vacinas;

LEIA-SE:

3.4.1.1.51. Minutos/horas desde a última atualização de vacinas. Em casos de soluções que não utilizam atualização de vacinas, a solução deve ter a capacidade de manter as funcionalidades e capacidades de detecção e prevenção sempre atualizadas através de uma conexão persistente com a arquitetura em nuvem do fornecedor;

ONDE SE LÊ:

3.4.1.1.54. Se é necessário reiniciar o computador para aplicar mudanças;

LEIA-SE:

3.4.1.1.54. Se é necessário reiniciar o computador para aplicar mudanças, ou indicar que a solução não tem necessidade de reboot para aplicar mudanças/atualizações;

ONDE SE LÊ:

3.4.1.1.58. Data e horário da última atualização de vacinas;

LEIA-SE:

3.4.1.1.58. Data e horário da última atualização de vacinas. Em casos de soluções que não utilizam atualização de vacinas, Data e horário da última conexão com a plataforma da solução;

ONDE SE LÊ:

3.4.1.1.81. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;

LEIA-SE:

3.4.1.1.81. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos ou em caso de solução SaaS, ser via conexão com a arquitetura em nuvem do fornecedor da solução;

ONDE SE LÊ:

3.4.1.1.82. Capacidade de herança de configuração de tarefas, políticas e relatórios na estrutura de hierarquia de servidores on-premisse com servidor em cloud;

LEIA-SE:

3.4.1.1.82. Capacidade de herança de configuração de tarefas, políticas e relatórios na estrutura de hierarquia de servidores on-premisse com servidor em cloud ou em caso de solução SaaS, ser via conexão com a arquitetura em nuvem do fornecedor da solução;

ONDE SE LÊ:

3.4.1.1.83. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;

LEIA-SE:

3.4.1.1.83. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede ou em caso de solução SaaS, ser via conexão com a arquitetura em nuvem do fornecedor da solução.

ONDE SE LÊ:

3.4.1.1.84. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;

LEIA-SE:

3.4.1.1.84. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo ou em caso de solução SaaS, ser via conexão com a arquitetura em nuvem do fornecedor da solução;

ONDE SE LÊ:

3.4.1.1.88. Capacidade exportar eventos para sistemas de SIEM no formato LEEF e CEF.

LEIA-SE:

3.4.1.1.88. Capacidade exportar eventos para sistemas de SIEM no formato LEEF ou CEF.

ONDE SE LÊ:

3.4.1.1.90. Dever ter a capacidade de exportar eventos para sistemas de SIEM, compatível com Qradar, ArcSight e Splunk.

LEIA-SE:

3.4.1.1.90. Dever ter a capacidade de exportar eventos para sistemas de SIEM, compatível com Qradar;

ONDE SE LÊ:

3.4.1.1.93. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;

LEIA-SE:

3.4.1.1.93. Deve encontrar computadores na rede através de no mínimo duas formas: Domínio e Active Directory;

ONDE SE LÊ:

3.4.2.4.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;

LEIA-SE:

3.4.2.4.8. Controle de acesso a sites por categoria, podendo também ser por meio de detecção de comportamento malicioso, com ou sem arquivos conhecidos ou desconhecidos;

ONDE SE LÊ:

3.4.2.4.15. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

LEIA-SE:

3.4.2.4.15. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa). Em casos de soluções que não utilizam atualização de vacinas, a solução deve ter a capacidade de manter as funcionalidades e capacidades de detecção e prevenção sempre atualizadas através de uma conexão persistente com a arquitetura em nuvem do fornecedor;

ONDE SE LÊ:

3.4.2.4.25. Deverá possuir módulo para proteção contra malwares que tenta realizar criptografia de arquivos em pastas compartilhadas.

LEIA-SE:

3.4.2.4.25. Deverá possuir módulo para proteção contra malwares que tenta realizar criptografia de arquivos;

ONDE SE LÊ:

3.4.2.4.59. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/);

LEIA-SE:

3.4.2.4.59. Deve possuir módulo de bloqueio de Phishing;

ONDE SE LÊ:

3.4.2.4.61. Deve possuir módulo para proteção contra port scans, network flooding e MAC spoofing. A base de dados de análise deve ser atualizada juntamente com as vacinas;

LEIA-SE:

3.4.2.4.61. Deve possuir módulo para proteção contra port scans, network flooding e MAC spoofing.

ONDE SE LÊ:

3.4.1.1.78. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;

LEIA-SE:

3.4.1.1.78. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes. Em caso de solução SaaS, que a gerência de redundância e balanceamento de carga sejam pela mesma;

ONDE SE LÊ:

3.4.1.1.79. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;

LEIA-SE:

3.4.1.1.79. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus. Em caso de solução SaaS, a capacidade de obter os relatórios será através da console da solução de maneira centralizada;

ONDE SE LÊ:

3.4.1.1.81. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;

LEIA-SE:

3.4.1.1.81. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos. Em caso de solução SaaS, que a capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos sejam pela mesma;

ONDE SE LÊ:

3.4.1.1.83. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;

LEIA-SE:

3.4.1.1.83. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede. Em casos de soluções que não utilizam atualização de repositórios de vacinas, a solução deve ter a capacidade de manter as funcionalidades e capacidades de detecção e prevenção sempre atualizadas através de uma conexão persistente com a arquitetura em nuvem do fornecedor;

ONDE SE LÊ:

3.4.1.1.84. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;

LEIA-SE:

3.4.1.1.84. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo. Em casos de soluções que não utilizam atualização de repositórios de vacinas, a solução deve ter a capacidade de manter as funcionalidades e capacidades de detecção e prevenção sempre atualizadas através de uma conexão persistente com a arquitetura em nuvem do fornecedor;

ONDE SE LÊ:

3.4.12.2.35. Deve permitir integrar com solução de SIEM por protocolo de syslog, através de encriptação usando TLS.

LEIA-SE:

3.4.12.2.35. Deve permitir integrar com solução de SIEM compatível com Qradar.

ONDE SE LÊ:

9.5.7.3. Número e vigência do contrato.

LEIA-SE:

9.5.7.3. Vigência do contrato.

Acerca das novas datas de realização da sessão pública do Edital de Pregão Eletrônico n. 28/2024:

RECEBIMENTO DAS PROPOSTAS ATÉ: 26/08/2024 às 10:00 horas (Horário de Brasília).

ABERTURA DAS PROPOSTAS: 26/08/2024 às 10:00 horas (Horário de Brasília).

INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS: 26/08/2024 às 10:30 horas (Horário de Brasília).

Maiores informações por meio do Portal do TJCE na internet (www.tjce.jus.br) ou pelo email cpl.tjce@tjce.jus.br.

Permanecem inalteradas as demais cláusulas e condições do referido Edital e seus Anexos.

Fortaleza, aos 31 de julho de 2024.

Denise Maria Norões Olsen
SECRETÁRIA DE TECNOLOGIA DA INFORMAÇÃO DO TJCE

Sérgio Mendes de Oliveira Filho
SECRETÁRIO-GERAL ADMINISTRATIVO DO TJCE

Aprovado:

Cristiano Batista da Silva
CONSULTOR JURÍDICO DA PRESIDÊNCIA DO TJCE