prodam

tecnologia da informação e comunicação

AQUISIÇÃO DE LICENÇA DO SOFTWARE NESSUS PROFESSIONAL

TERMO DE REFERENCIA

DIRETORIA DE INFRAESTRUTURA E TECNOLOGIA

Janeiro / 2019

Wagner Kanagusuko
Coordenador do Núcleo de Segurança
RF: 15.834-0

EMPRESA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO MUNICÍPIO DE SÃO PAULO - PRODAM-SP S/A
Av. Francisco Matarazzo, 1500 - Torre Los Angeles - Água Branca - CEP 05001-100 - São Paulo - SP
Tel.: (11) 3396-9000 - Fax: (11) 3396-9001

TERMO DE REFERÊNCIA

1. OBJETO

1.1. Aquisição de 01 (uma) licença do software Tenable Nessus Professional com validade de 01 (um) ano; utilizado como scanner de vulnerabilidade e auditoria de segurança de redes.

2. ESPECIFICAÇÃO TÉCNICA

2.1. O software deve prover, no mínimo, as seguintes funcionalidades:

2.1.1. Em relação a recursos de análise:

2.1.1.1. Criação de políticas de varredura;

2.1.1.2. Possibilitar o agendamento de *scans*;

2.1.1.3. Escaneamento sem agentes para facilitar um *scan* eventual;

2.1.1.4. Programação de *scans* para rodar uma única vez ou de forma recorrente;

2.1.1.5. Realizar avaliações de vulnerabilidade contra uma ampla variedade de sistemas;

2.1.1.6. Arquitetura *plug-in* permitindo que usuários personalizem-no para seus sistemas e redes;

2.1.1.7. Busca de vulnerabilidades em tempo real;

2.1.1.8. Grande base de vulnerabilidade e *plug-ins*;

2.1.1.9. Modelos pré-configurados de *scan*;

2.1.1.10. *Scanner* (varredura) de rede para identificar portas TCP/UDP abertas.

Wagner Kanagusuko
Coordenador do Núcleo de Segurança
RF 15.834-0

2.1.2. Em relação a recursos de implementação:

2.1.2.1. Gerenciamento centralizado de múltiplos Nessus;

2.1.2.2. Implantação e administração distribuída.

2.1.3. Em relação a recursos de relatório:

2.1.3.1. *Dashboard* de resultados;

2.1.3.2. Resultados atualizados após *plugin update*;

2.1.3.3. Classificar as vulnerabilidades pelo nível de criticidade;

2.1.3.4. Apresentar a descrição da vulnerabilidade, seu impacto e sua correção;

2.1.3.5. Visualização de problemas por categoria;

2.1.3.6. Cinco níveis de severidade: *Critical, High, Medium, Low, Info*;

2.1.3.7. Riscos baseados na pontuação CVE (*Common Vulnerabilities and Exposures*);

2.1.3.8. Geração de relatórios flexível: Customizar relatórios por tipo de vulnerabilidade ou *host*, criar Sumário Executivo ou comparar relatórios para evidenciar mudanças;

2.1.3.9. Gerar relatório nos formatos XML, PDF, CSV e HTML;

2.1.3.10. Envio de email com os resultados dos *scans*, recomendações de remediação e melhorias;

2.1.3.11. Compartilhamento dos resultados – Relatórios.

2.1.4. Em relação a recursos de controle de acesso:

2.1.4.1. Controle de acesso baseado em perfis;

2.1.4.2. Autenticação LDAP;

2.1.4.3. Facilidade na criação de perfis;

2.1.4.4. Configuração e gerenciamento via GUI (*Graphical User Interface*).

3. DO PRAZO DE ENTREGA

Wagner Kanagusuko
Coordenador do Núcleo de Segurança
RF: 15.834-0

3.1. O prazo máximo de entrega do software e suas licenças será de 30 (trinta) dias corridos, contados a partir da data de assinatura do contrato.

4. VIGÊNCIA

4.1. O contrato terá a vigência de 12 meses a partir da assinatura do contrato, podendo ser renovado até o limite legal. Durante este período estarão inclusas todas as atualizações de versões em toda solução.

5. OBRIGAÇÕES DA CONTRATADA

5.1. A Contratada deverá oferecer as licenças do software e suas funcionalidades contratadas por um prazo mínimo de 12 (doze) meses, a contar da data de sua efetiva instalação;

5.2. Disponibilizar profissional certificado pelo fabricante para ativação dos produtos contratados;

5.3. Disponibilizar número de telefone (local ou DDG) para suporte telefônico (24x7x365) e abertura de chamados técnicos;

5.4. O tempo máximo de atendimento para os chamados de defeitos deverá ser de 4 h (quatro horas) e de solução em até 6 h (seis horas) a contar do registro de abertura do chamado no Centro de Atendimento Técnico da Contratada, realizando testes e corrigindo defeitos sem ônus para a CONTRATANTE, durante o período de garantia;

6. DOCUMENTAÇÃO TÉCNICA

Wagner Kanagusuko
Coordenador do Núcleo de Segurança
RF: 15.834-0

6.1. Deverão ser fornecidos juntamente com o software e as licenças os manuais técnicos de referência, contendo todas as informações sobre o produto com as instruções para instalação, configuração e operação, preferencialmente em Português (Brasil), ou, na inexistência de tradução em Português, podem ser escritos em Língua Inglesa.

7. CONFIDENCIALIDADE

7.1. A CONTRATADA deverá zelar pelo sigilo de quaisquer informações referentes à estrutura, sistemas, usuários, contribuintes, topologia, e ao modo de funcionamento e tratamento das informações da CONTRATANTE, durante e após fim do contrato, salvo se houver autorização expressa da CONTRATANTE para divulgação.

7.2. Não haverá nenhum tipo de facilidade de acesso remoto, tão menos envio de forma automática ou controlada de informações (backdoor) originadas do software/hardware contratado ou adquirido sem o conhecimento e formal autorização da Contratante. A não observância a esse fato poderá ser considerada espionagem e será motivo de processo civil e criminal conforme legislação vigente.

São Paulo, 22 de Janeiro de 2019.

Mauricio Hanashiro
Gerência de Telecomunicações - GIC

Wagner Kanagusuko
Coordenador do Núcleo de Segurança
RF: 15.834-0