ERRATA Nº 01/2022

Nº do Processo: 004005-00605
Licitação: Pregão Eletrônico n° 0079/2022
Área Técnica Responsável: Gerência Corporativa de Tecnologia e Segurança da Informação
Objeto: Contratação de solução para gestão de vulnerabilidades e auditoria de configuração de ativos de rede, endereços IP, contêineres, ativos em nuvem e aplicações web, assim como serviços de instalação, suporte técnico, atualização e treinamento, pelo período de 36 meses

Belo Horizonte, 10 de outubro de 2022

A Comissão Permanente de Licitação, no desempenho de suas atribuições, comunica aos interessados a seguinte alteração:

- Para o item 3.3.1 do Anexo I – Termo de Referência

Onde se lê:

A solução deve ser entregue como um serviço Software-as-a-Service (SaaS) e ou híbrido em uma nuvem proprietária do fabricante para todos os seus serviços e aplicativos exigidos neste documento. Serviços fornecidos por nuvens de terceiros não são aceitos e também 100% on-primises.

Todos os serviços da plataforma devem estar disponíveis sob o mesmo padrão de qualidade de serviço 24x7x365 e garantir 99% de disponibilidade.

O ofertante deve oferecer manutenção e atualização constante da plataforma durante todo o período de vigência do contrato de serviço.

As atualizações de serviço devem ser transparentes para o administrador da solução, sem afetar nenhum dos dados armazenados - serviços fornecidos.

Será admitida apenas 1 desconexão por trimestre, por período de tempo não superior a 4 horas do serviço oferecido em janelas de manutenção programada e previamente avisado.

Todas as comunicações entre componentes, transferência de dados e sincronização da solução devem ser criptografadas de ponta a ponta, fazendo uso de no mínimo TLS 1.2, certificados assinados com RSA 2048 bits e algoritmo de assinatura SHA256.

Leia-se:

A solução deve ser entregue como um serviço Software-as-a-Service (SaaS) e ou híbrido em uma nuvem proprietária do fabricante para todos os seus serviços e aplicativos exigidos neste documento. Serviços fornecidos por nuvens de terceiros com total isolamento de tenants serão aceitos. Não serão aceitos ambiente 100% on-primises.

Todos os serviços da plataforma devem estar disponíveis sob o mesmo padrão de qualidade de serviço 24x7x365 e garantir 99% de disponibilidade.

O ofertante deve oferecer manutenção e atualização constante da plataforma durante todo o período de vigência do contrato de serviço.

As atualizações de serviço devem ser transparentes para o administrador da solução, sem afetar nenhum dos dados armazenados - serviços fornecidos.

Será admitida apenas 1 desconexão por trimestre, por período de tempo não superior a 4 horas do serviço oferecido em janelas de manutenção programada e previamente avisado.

Todas as comunicações entre componentes, transferência de dados e sincronização da solução devem ser criptografadas de ponta a ponta, fazendo uso de no mínimo TLS 1.2, certificados assinados com RSA 2048 bits e algoritmo de assinatura SHA256.

- Para o item 3.3.2 do Anexo I – Termo de Referência

Onde se lê:

A solução proposta deverá permitir a descoberta e o inventário de todos os ativos conhecidos e desconhecidos que se conectam ao ambiente de TI híbrido (global) da organização, incluindo dispositivos e aplicativos móveis locais, estações de trabalho, servidores, dispositivos de rede / telecomunicações / segurança, nuvens, contêineres, TO e IoT.

Leia-se:

A solução proposta deverá permitir a descoberta e o inventário de todos os ativos conhecidos e desconhecidos que se conectam ao ambiente de TI híbrido (global) da organização, incluindo dispositivos e aplicativos móveis locais, estações de trabalho, servidores, dispositivos de rede / telecomunicações / segurança, nuvens, contêineres e IoT.

- Para o item 4.1.18 do Anexo I – Termo de Referência

Onde se lê:

A Solução deve possibilitar a análise das aplicações WEB com as seguintes características:

- *Habilitar varreduras profundas dinâmicas para descobrir e catalogar todos os aplicativos da web e APIs na rede corporativa externa, redes corporativas internas e instâncias de nuvem.*
- *Permitir varreduras autenticadas, complexas e progressivas.*
- *Suportar varreduras programadas de serviços SOAP e REST API.*
- *Contar com uma API e integração com Jenkins para automação em um ambiente de CI / CD.*
- *Detectar, identificar, avaliar, rastrear e corrigir os 10 principais riscos OWASP (Top 10), como injeção de SQL, Cross-site script (XSS), XML External Entity (XXE), autenticação interrompida e configurações incorretas, também ameaças de WASC, vulnerabilidades CWE e CVEs associados em aplicações da web.*
- *Suportar a capacidade de re-testar uma vulnerabilidade específica que foi detectada anteriormente na aplicação web.*
- *Gerar tags para facilitar a localização e o uso de ativos de aplicações web encontrados.*
- *Permitir que se faça a varredura de grandes aplicações da web usando um mecanismo de varredura progressiva, que deve permitir a varredura em estágios incrementais e evitar quaisquer restrições que possam surgir ao tentar fazer a varredura de um aplicativo de uma vez.*
- *Definir a hora exata de início e duração das verificações.*

- *Permitir gerenciar várias varreduras de aplicações web, combinando vários scanners para acelerar o processo e obter resultados mais rapidamente.*
- *Consolidar os dados de varredura automatizada da solução com dados de ferramentas que permitem a avaliação manual de vulnerabilidades por meio do Burp Suite e Bugcrowd, para uma visão unificada de vulnerabilidades de aplicações web detectadas automática e manualmente.*

Leia-se:

A Solução deve possibilitar a análise das aplicações WEB com as seguintes características:

- *Habilitar varreduras profundas dinâmicas para descobrir e catalogar todos os aplicativos da web e APIs na rede corporativa externa, redes corporativas internas e instâncias de nuvem.*
- *Permitir varreduras autenticadas, complexas e progressivas.*
- *Suportar varreduras programadas de serviços SOAP e REST API.*
- *Contar com uma API e integração com Jenkins para automação em um ambiente de CI / CD.*
- *Detectar, identificar, avaliar e rastrear os 10 principais riscos OWASP (Top 10), como injeção de SQL, Cross-site script (XSS), XML External Entity (XXE), autenticação interrompida e configurações incorretas, também ameaças de WASC, vulnerabilidades CWE e CVEs associados em aplicações da web.*
- *Suportar a capacidade de re-testar uma vulnerabilidade específica que foi detectada anteriormente na aplicação web.*
- *Gerar tags para facilitar a localização e o uso de ativos de aplicações web encontrados.*
- *Permitir que se faça a varredura de grandes aplicações da web usando um mecanismo de varredura progressiva, que deve permitir a varredura em estágios incrementais e evitar quaisquer restrições que possam surgir ao tentar fazer a varredura de um aplicativo de uma vez.*
- *Definir a hora exata de início e duração das verificações.*
- *Permitir gerenciar várias varreduras de aplicações web, combinando vários scanners para acelerar o processo e obter resultados mais rapidamente.*

Consolidar os dados de varredura automatizada da solução com dados de ferramentas que permitem a avaliação manual de vulnerabilidades por meio do Burp Suite e Bugcrowd, para uma visão unificada de vulnerabilidades de aplicações web detectadas automática e manualmente.

As demais condições do Edital permanecem inalteradas.

Diante da alteração acima, considerando a possibilidade de afetar e ampliar a formulação das propostas, fica redesignada a data de abertura da sessão para o dia **25/10/2022 às 09:00h**.

JOSIANE CALDEIRA ALVES:07992040643
Assinado de forma digital por JOSIANE CALDEIRA ALVES:07992040643
Dados: 2022.10.10 08:47:20 -03'00'

Josiane Caldeira Alves
Comissão Permanente de Licitação do Sesc em Minas