Resposta a Pedido de Esclarecimento

QUESTIONAMENTOS:

Item 9.1.14: Para o cadastro de ativos, é correto inferir que a ferramenta deverá prover meios de fazer o cadastro manual via entrada manual, importação de lista de ativos em arquivo texto, discovery via varredura de DNS ou ICMP, ou ainda por meio de diretórios LDAP. Está correto o entendimento?
RESPOSTA: Sim.

Item 9.1.14: Entendemos ainda que, no cadastro de ativos, para prover qualquer tipo de registro adicional e automático, a solução deverá permitir o cadastramento via API (seja REST ou SOAP) para facilitar a integração soluções adicionais. Está correto nosso entendimento?
RESPOSTA: Não, pois a especificação não descreve esses itens como obrigatórios. Podem estar acoplados à solução, porém não serão obrigatórios.

Item 9.1.15: Entendemos que a criação de grupo de ativos personalizados deverá também ser feita de maneira independente, ou seja, com a gestão de controle acesso de usuários distintos e permitindo também a hierarquização destes grupos, ou seja, por exemplo, departamento de informática com sub-grupos de Banco de Dados, Infraestrutura e Desenvolvimento. Nosso entendimento está correto?
RESPOSTA: A criação de grupos deve ser independente, permitindo pelo menos 3 classificações.

Item 9.1.17: Em caso do contratante desejar implementar varreduras em localidades físicas, servidores e redes distintos, a solução não
deveria permitir a implementação de múltiplas instâncias de servidores de scan e controladas a partir do servidor central. Está correto o
entendimento?
RESPOSTA: A Solução poderá permitir a instalação de múltiplas instâncias, porém isso não constitui um requisito para o scan em localidades fisicamente
distantes porém acessíveis via rede.

Item 9.1.22: Nosso entendimento de varreduras fisicamente separadas se estender a visão de vulnerabilidades sob o conceito de um “atacante externo”, a solução deverá permitir a integração com pelo menos um provedor de infraestrutura de nuvem, seja Azure, AWS ou Google, permitindo que uma instância virtual seja criada nesse provedor automaticamente para rodar um scan a partir da Internet gerindo vulnerabilidades de acessos externos, nosso entendimento está correto?
RESPOSTA: Não há essa necessidade prevista no edital.

Item 9.1.22: No caso de permitir múltiplas instâncias para rodar o scan, o usuário deverá ter capacidade de escolher o servidor ou grupo de servidores que irão rodar o scan, de maneira a controlar a origem de onde irá partir a varredura a partir da gerencia, nosso entendimento está correto?
RESPOSTA: Não há essa necessidade prevista no edital.

Item 9.1.18: Entendemos que o armazenamento de resultados de forma cifrada no servidor de scan são um requisito caso esses dados não possam ser completamente removidos (apagados) e transferidos de maneira sumarizada, controlada e segura para o Banco de dados central da ferramenta de gerência, nosso entendimento está correto?
RESPOSTA: Os resultados devem ser armazenados de maneira cifrada, independente do local de armazenamento.

Item 9.1.27: No caso de aplicações que possuem restrição ao crawling (autenticação ou navegação restrita), estamos entendendo que a ferramenta deveria ter capacidade de receber os casos de uso da aplicação, incluindo credenciais de autenticação para o autopreenchimento de formulários web(durante a navegação), lista de urls a serem navegadas, exportação de ferramentas de QA tipo Chrome HAR, Selenium ou Burp Proxy, nosso entendimento está correto?
RESPOSTA: Não há essa necessidade prevista no edital.

Item 9.1.41: Estamos entendendo que a existência de credencias com capacidade de administração para executar novos scans ou alterara gendamento, bem como credenciais de visualização, que não tenham essa capacidade, já seria o suficiente para controlar tarefas críticas no sistema, nosso entendimento está correto?
RESPOSTA: Sim.

Item 9.1.37: Nosso entendimento para este item e que a funcionalidade de criação de ticket deve estar integrada automacatimente com o fabricante, de maneira a permitir o suporte técnico para correção e ao apoio específico no processo de mitigação de riscos, nosso entendimento está correto?
RESPOSTA: Não necessariamente ao fabricante, mas sim à equipe responsável pelo ativo.

Item 9.1.43: Independente do volume comercial determinado pela contratante de IPs (4096) e URLs(100), a solução não deveria ter capacidade técnica indefinida de adicionar novos endereços IPs ouURLs, permitindo que o contratante possa escalar o serviço de acordo com suas necessidades, nosso entendimento está correto?
RESPOSTA: Essas quantidades são mínimas, portanto, suportando uma capacidade maior de endereços, não haveria nenhum problema em aceitar.