QUESTIONAMENTO 4

Referência: PREGÃO ELETRÔNICO 92/2013

Objeto: aquisição de Solução de gerenciamento de eventos de segurança da informação (SIEM - Security Information and Event Management).

1. "O presente contrato tem por objeto o fornecimento de Solução de gerenciamento de eventos de segurança da informação (SIEM - Security Information and Event Management), incluindo serviços de suporte técnico na modalidade On-Site, com suporte técnico de 36 meses, instalação, configuração e transferência de conhecimento e treinamentos oficiais do fabricante. Esta solução composta por Hardware, Software, serviços, garantia e suporte técnico. Para atendimento à legislação tributária vigente, hardware, software e serviços não podem constar da mesma fatura devido a incidência distinta de tributos. Desta forma, entendemos que, hardware deve ser faturado como produto com a correspondente incidência dos tributos pertinentes, licenças de software deve ser faturado como produto com a correspondente incidência dos tributos pertinentes e serviços devem ser faturados como serviços com a correspondente incidência dos tributos pertinentes. Está correto nosso entendimento?

   Resposta: Está correto o entendimento. Ademais, o faturamento da solução, indubitavelmente, deverá seguir a legislação vigente, no que tange o tipo de cada item fornecido e sua incidência tributária.

2. "Questionamento ao ITEM - 4.30 : A solução deve ser capaz de identificar malwares e ataques do tipo "Zero Day". Entendemos que a detecção de mallwares e ataques do tipo "zero-day" somente é possível através da extração dos objetos maliciosos e análise de padrões de comunicação de rede, portanto é esperado que a solução do proponente suporte nativamente a captura de pacotes de rede, armazenamento, interpretação e extração destes objetos para realizar a análise. É correto o nosso entendimento?"

   Resposta: Não está correto o entendimento. A solução deve identificar malwares e ataques do tipo "zero-day" através da análise dos logs que foram coletados, ou seja, esta identificação se baseia na análise dos logs de diversas aplicações (item 4.19) e que a solução seja capaz de alertar de que algo incomum (com base no que já foi analisado pela solução anteriormente) está ocorrendo ou ocorreu. A análise de pacotes de rede não é necessária.

3. "Questionamento ao **ITEM - 4.30** : com relação ao questionamento anterior Entendemos que a detecção de mallwares e ataques do tipo "zero-day" deverá obrigatoriamente utilizar mecanismos como execução do objeto malicioso em sandbox local, sanbox na nuvem (Ex. ThreatGrid), checagem com provedores de anti-virus e inteligencia da comunidade externa (Ex. Virus Total) de forma nativa na solução do proponente. É correto o nosso entendimento?"

   Resposta: Conforme esclarecido no questionamento anterior, a identificação de malwares e ataques "zero-day" é com base na análise de logs correlacionados, não de pacotes de rede, o que torna desnecessária a utilização de sandboxes e checagens externas a provedores. A base para comparação dos registros de atividades suspeitos, quando necessária, deverá ser nativa da solução, não devendo a solução acessar diretamente bases de terceiros, mantidas pela comunidade e provedores externos, tampouco dependendo de licenciamento específico para acesso a qualquer base que se fizer necessária. Havendo necessidade de licenciamento de acesso e atualização, o mesmo deverá estar contemplado na proposta e terá a validade determinada no edital com relação ao suporte técnico.

Paulo Gerva

Pregoeiro