QUESTIONAMENTO 3

Referência: PREGÃO ELETRÔNICO 88/2013

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

1. "No subitem "4.19", que exige a coleta, de forma nativa, para diversos padrões. Dentre eles, na alínea l, é exigido o suporte ao banco de dados Postgres. Sendo o PostgreSQL um sistema de banco de dados livre, que grava seus eventos em syslog, entendemos que, para que haja competitividade poderemos comprovar este item através da comprovação do suporte ao padrão syslog. Estamos corretos no nosso entendimento?
   Resposta: Está correto o entendimento se, e somente se, a solução ofertada prover o mecanismo de coleta e interpretação correta dos campos da log para o banco de dados Postgres, sem a intervenção do administrador da ferramenta para prévia configuração das logs no sistema.

2. "No subitem "4.19", que exige a coleta, de forma nativa, para diversos padrões. Dentre eles, na alínea o, é exigido o suporte ao produto Cisco Wireless Connector System. Fizemos uma consulta na internet e não encontramos nenhuma referência ao nome "Cisco Wireless Connector System". Encontramos "Cisco Wireless LAN Controllers". Portanto, tentendemos que poderemos comprovar esse item através do suporte ao produto "Cisco Wireless LAN Controllers". Estamos corretos no nosso entendimento?"
   Resposta: Sim, está correto o entendimento.

3. "No subitem "4.19", que exige a coleta, de forma nativa, para diversos padrões. Dentre eles, na alínea q, é exigido o suporte aos produtos McAfee ePolicy Orchestrator e VirusScan Enterprise. Sendo ePolicy Orchestrator a console central do McAfee VirusScan Enterprise, entendemos que para que não haja redundância de informação, poderão ser aceitas soluções que suportem de forma nativa o McAfee ePolicy Orchestrator ou o McAfee Virus Scan Enterprise . Estamos corretos no nosso entendimento?"
   Resposta: A solução deverá, obrigatoriamente, suportar o padrão das logs geradas pelo McAfee ePolicy Orchestrator.

4. "No subitem "4.21" é exigida que a solução deva "...possuir a funcionalidade de envio de e-mails automáticos, sms e trap-snmp". Trabalhamos com solução líder mundial em SIEM e não trabalhamos com comunicação SMS. Entendemos que, para que haja competitividade, a funcionalidade de envio de SMS poderá ser considerada desejável porém não obrigatória. Estamos corretos no nosso entendimento?"
   Resposta: Não está correto o entendimento. A solução deverá fornecer ao menos uma integração com um servidor SMS, seja pela disponibilização de uma interface gráfica nativa, seja pela utilização de ferramenta auxiliar, cujo envio seja disparado através da execução de um comando de forma automática.

5. "No subitem "4.27" é exigido que a "...solução deve possuir a capacidade de se adaptar a eventos e melhorar as respostas futuras". Por esse item ser de difícil comprovação, entendemos que a sua comprovação poderá ser feita através das funcionalidades de análise de comportamento de rede. Estamos corretos no nosso entendimento?"
   Resposta: Sim, está correto o entendimento. O atendimento a esse item poderá ser feito dessa forma.

6. "No subitem "5.5" é exigido que a "...deve ser capaz de coletar logs e eventos de quaisquer dispositivos e aplicações IP que suportem nativamente os protocolos: SYSLOG, SYSLOG-NG, SNMP, Microsoft Windows Event Logging API, Microsoft Windows Remote Management, Microsoft Windows RPC, FTP, arquivos de logs texto formatados (vírgula/tabulação/delimitado), ODBC". A nossa solução, líder de mercado de SIEM consegue atender a todos os requisitos exigidos, no entanto, referente aos diversos "padrões" listados pela Microsoft conseguimos comprovar, apenas, a coleta em um dos formatos mencionados. Portanto, acreditamos que poderão ser aceitas soluções que suportem a coleta de eventos de pelo menos um dos 3(três) métodos de coletas de eventos Microsoft Listados, sem nenhum prejuízo ao certame. Estamos corretos no nosso entendimento?"
   Resposta: Está correto o entendimento se, e somente se, a solução ofertada suportar nativamente, no mínimo, o Microsoft Windows Event Logging API, uma vez que os demais serviços da Microsoft suportam o envio de suas logs para a referida API.

7. "No subitem "5.15", é exigido que a solução deva "...comprimir os eventos antes do envio aos correlacionadores". Por trabalhar com solução que incorpora todas as funcionalidades (coleta de eventos, correlacionamento de eventos e console de gerência) em um único equipamento, entendemos que essa funcionalidade deva ser considerada desejável, porém, não obrigatória. Estamos corretos no nosso entendimento?"
   Resposta: Sim, está correto o entendimento, em se tratando de solução única que incorpora todas as funcionalidades.

8. “No subitem “6.14”, é exigida que a solução seja capaz de, “...executar ações automáticas como: executar script, enviar e-mail, enviar SMS, enviar mensagem para o usuário...”. Trabalhamos com solução líder de mercado de SIEM, que por entender ser arriscado tomar medidas automáticas, não permite a execução, de scripts e por conseguinte, o envio de SMS. Portanto, para que haja competitividade a esse certame, entendemos que essas funcionalidades (envio de SMS e execução de Script) devam ser consideradas desejáveis, porém, não obrigatórias. Estamos corretos no nosso entendimento?”
   Resposta: Não está correto o entendimento. A solução, como um todo, deverá ser capaz de executar ações automáticas definidas pelo administrador, com base no resultado de aplicações de regras de correlacionamento.

Paulo Gerva

Pregoeiro