QUESTIONAMENTO 3

Referência: PREGÃO ELETRÔNICO 92/2013

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

1. "Item 5.7 A solução deve ser capaz de armazenar os dados localmente (cache), caso os correlacionadores estejam indisponíveis. Deve permitir a configuração do tamanho do cache;
   Questionamento item 5.7:
   Limitar o tamanho do cache em caso de indisponibilidade do correlacionador, compromete negativamente o gerenciamento de segurança em um ambiente, uma vez que importantes eventos poderão ser descartados em caso de preenchimento total do cache, mesmo que haja disco/armazenamento fisicamente disponível. Por tal motivo, entendemos que a melhor prática seja disponibilizar o total de armazenamento disponível nos coletores para cache de eventos, ao invés de limitar tal espaço quando se tem ainda disponibilidade de tal recurso, visando assim um menor risco de se perder importantes eventos. Entendemos ainda, que a maior preocupação da exigência do item 5.7 é justamente a garantia de não se perder eventos relevantes, fazendo com que a configuração do tamanho do cache nesse caso, seja desnecessária e não desclassificatória em caso de não cumprimento. Além do que estaremos oferecendo solução do tipo distribuída na qual contaremos com equipamento do tipo Appliance, responsável pela coleta de eventos e envio ao correlacionador, dimensionado de acordo com a necessidade de EPS exigida no edital. Nosso entendimento está correto?"

   Resposta: Está correto o entendimento se, e somente se, a solução garantir que o livre crescimento da cache armazenada não compromete a estabilidade do sistema operacional em execução, por meio de, por exemplo, a separação dos discos de sistema e dados.

2. "Item 5.9 A solução deve ser capaz de ajustar o horário dos eventos, caso necessário, com base em limites de diferença de hora entre os eventos originais e a hora correta obtida pelo sistema através de protocolo NTP com os servidores locais;
   Questionamento item 5.9
   Um dos valores mais importantes de um LOG e consequentemente, de um evento, é o instante de seu acontecimento. Alterar tais valores compromete toda a integridade de administração e gerenciamento dos eventos, sua correlação e geração de alertas e relatórios, bem como toda a precisão de rastreabilidade de um determinado fato. Entendemos ainda, que um servidor de NTP bem configurado é pré-requisito para instalação de qualquer solução de SIEM, para que os eventos tenham seus instantes de ocorrência corretos e em conformidade com o relógio da rede em questão. A solução de SIEM ofertada deverá apenas ajustar diferenças de time-zones, caso os eventos sejam coletados de diferentes fusos. Caso haja divergência entre o horário do evento original coletado e o time zone definido para o ativo, alertas serão enviados para a console de gerenciamento, para que o ajuste de time zone seja realizado, mantendo a originalidade/integralidade do evento coletado. Nosso entendimento está correto?"

   Resposta: Não está correto o entendimento. Além do ajuste de fuso horário, a aplicação deve ser capaz de ajustar, se necessário, de modo a auxiliar a correlação, horários de logs de aplicações e dispositivos legados que não estejam sincronizados com NTP.

3. "Item: 6.8 O correlacionador deve permitir a execução das regras agendadas, que executam em frequência e horário específico, sem ficarem ativas em tempo real;
   Questionamento Item 6.8:
   Entendemos que as regras devem estar ativas constantemente, podendo utilizar o tempo de acontecimento dos eventos como parte da regra de análise e correlação, sem a necessidade de desativá-la. Esta preocupação de desativar regra relaciona-se a performance do correlacionador de eventos. Nossa solução é do tipo distribuída com equipamento tipo Appliance específico para a funcionalidade de correlacionamento, sendo que o mesmo foi dimensionado para atender ao requisito de EPS exigido neste edital. Nosso entendimento está correto?"

   Resposta: Não está correto o entendimento. A solução deve permitir que determinadas regras possam ser agendadas para efetuarem a correlação em horários pré-definidos. Sabe-se a dimensão de eventos para o correlacionamento, mas não a quantidade e desempenho das regras de correlacionamento que serão definidas. Dessa forma, a funcionalidade é necessária.

4. "Item: 6.12 O correlacionador deve detectar e desativar automaticamente regras que estejam gerando loop infinito com base num mesmo evento ou alerta;
   Questionamento Item 6.12:

Nossa solução correlaciona os eventos normalizados e todas as regras são construídas através de console específica para este fim. Por este motivo na nossa solução este tipo de problema não ocorre, visto que esta necessidade é atendida nativamente.
Está correto nosso entendimento?"

Resposta: Está correto o entendimento se, e somente se, houver comprovação de que o console alerta ou não permite a criação de regras que possam gerar loops.

5. "Item: 6.13 O correlacionador deve detectar e desativar temporiariamente e de forma automática regras que estejam gerando número excessivo de alertas num curto espaço de tempo, visando proteger o sistema contra ataques onde se tenta inundar a interface com alertas para ocultar outros ataques em andamento.
Questionamento item 6.13:
Nossa solução correlaciona eventos normalizados e todas as regras são feitas através de console específica construída para este fim. Ofereceremos solução distribuída com equipamento do tipo Appliance responsável pela coleta de eventos e normalização dos eventos. Este equipamento possui mecanismo de proteção garantindo que somente os ativos cadastrados estão autorizados a enviar eventos para o Appliance. Portanto este mecanismo não se faz necessário na nossa solução e, ao mesmo tempo, este tipo de mecanismo pode gerar uma ideia errônea de normalidade no ambiente para o mecanismo de correlacionador de eventos.
Está correto o nosso entendimento?"

Resposta: Está correto o entendimento se, e somente se, houver comprovação de que a solução ofertada evita ou mesmo controla esse tipo de ataque.

Paulo Gerva

Pregoeiro