RESPOSTA AO 2º PEDIDO DE ESCLARECIMENTO DA EMPRESA L.M. ROCHA CONSULTORIA – (PE-RP N° 017/2024)

Nos termos do edital supracitado, vimos fazer os seguintes esclarecimentos, especificamente em relação ao CATÁLOGO DE SERVIÇOS da Operação Assistida, previsto no item 3.10.2.11 do Termo de Referência.

Questionamento 01:

Em relação à "Inclusão de coleta em banco de dados" (item1), entendemos que refere-se a expansão da base de monitoramento através da inserção/integração de novas fontes de dados. Está correto?

RESPOSTA: Sim, o entendimento está correto.

Questionamento 02:

Sobre a "Ampliação de espaço" (item 8), entendemos que se refere à expansão da base de monitoramento através da inserção/integração de novas fontes de dados. Está correto?

RESPOSTA: O entendimento está parcialmente correto. O referido item é destinado à ampliação do espaço cibernético de interesse, onde o Contratante poderá solicitar a inclusão de fontes de dados localizadas na deep web e dark web.

Questionamento 03:

Acerca da "Inclusão de coleta de vulnerabilidade" (item 11), deve-se considerar o gerenciamento de vulnerabilidades para um escopo total aproximado de quantos ativos e quantas aplicações?

RESPOSTA: Uma vez que o processo trata de uma Ata de registro de preços, onde há a intenção de contratação pelos órgãos participantes, o quantitativo total estimado encontra-se na tabela do tópico 2.2.6. do Termo de Referência.

Questionamento 04:

No "Desenvolvimento de integração" (item 13), compreende-se que esta tarefa está relacionada à capacidade de ingestão dos logs das tecnologias mencionadas, ou ao envio de dados/informações para essas tecnologias, a fim de poderem executar ações de remediação. Está correto?

RESPOSTA: Sim, o entendimento está correto.

Questionamento 05:

Na "Integração específica" (item 14), solicitamos que sejam mencionados exemplos de possíveis soluções para integração, assim como a quantidade total estimada.

RESPOSTA: No item 14 do catálogo de serviços, é esperado que a Contratada execute a integração da solução com ferramentas como por exemplo: Firewall, EDR e SIEM. Novamente, por tratar-se de uma Ata com a adesão de diversos órgãos, não há como prevermos, especialmente no primeiro ano de contratação, a quantidade de acionamentos deste item do catálogo.

Questionamento 06:

Na tarefa de "Notificação automática de ativo do escopo envolvido em download de conteúdo em redes p2p" (item 33), pergunta-se:

a) Qual seria o objetivo principal desta tarefa: identificar menções a dados supostamente relacionados ao PRODERJ em compartilhamentos realizados via BitTorrent ou plataformas similares, como fóruns de compartilhamento e venda de dados, ou verificar a utilização desses mecanismos de compartilhamento por usuários em dispositivos internos?

RESPOSTA: O objetivo é monitorar possíveis ameaças ao escopo de monitoramento dos órgãos contratantes, e no caso do item 33 do catálogo, deve ser monitorada a rede BitTorrent, de modo que seja detectado qualquer tráfego dos ativos do escopo nessa rede, e então realizada a notificação imediata, constando o IP de origem desse arquivo e o tipo de conteúdo.

b) Em caso do foco ser a identificação da utilização deste mecanismo em ativos internos, qual seria o escopo total (quantidade) aproximado de ativos envolvidos?

RESPOSTA: O referido item do catálogo não trata do monitoramento de usuários e ativos internos, mas sim dos ativos expostos na internet.