17359631 08006.000003/2021-38

Ministério da Justiça e Segurança Pública
Secretaria-Executiva
Coordenação de Riscos e Segurança de TIC

RESPOSTA AO PEDIDO DE ESCLARECIMENTO 13 - CRS

1. Trata-se de resposta ao pedido de esclarecimento nº 13 (17357810) ao edital do Pregão Eletrônico nº 21/2021, cujo objeto é a contratação de empresa especializada, para o fornecimento de **Serviço de Centro de Operações de Segurança (Security Operations Center - SOC) com funcionamento e suporte 24h por dia e 7 dias por semana, Serviço de tratamento e resposta aos incidentes cibernéticos - CSIRT - Blue Team e Serviço de teste de invasão - Red Team,** pelo período de 24(vinte e quatro) meses, renováveis até o limite de 60 (sessenta) meses, para o atendimento das necessidades da Diretoria de Tecnologia da Informação e Comunicação - DTIC do Ministério da Justiça e Segurança Pública - MJSP, conforme informações constantes do Edital (17308596).

2. No referido pedido de esclarecimento foi feito um questionamento de ordem técnica. Abaixo segue a resposta ao questionamento.

2.1. Esclarecimento 1 -

> a) Referente ao atestado de capacidade técnica, item 12.3.1.1.1 do TR, estamos entendendo que serão aceitos atestados que comprovem a prestação de serviços antivírus de gateway, Anti-Malware, Next Gen Antivirus (NGAV) ou EDR (Endpoint Detection and Response). Está correto o nosso entendimento?

2.2. Resposta: Não, o entendimento está incorreto. O item 12.3.1.1.1 NÃO se refere a prestação de serviços antivírus, anti-malware ou Next Gen Antivírus. Quanto ao EDR, é solicitado a experiência na prestação de serviços de administração de solução de análise e correlacionamento Monitoramento de estação de trabalho (Endpoint Detection and Response - EDR), conforme item 12.3.1.1.1. do Termo de Referência do Ministério da Justiça e Segurança Pública:

> 12.3.3.1.1. Experiência na prestação de serviços de administração de solução(ões)
> de automação (Orquestração, Automação e Resposta deSegurança (Security Orchestration, Automation, and Response - SOAR),
> de análise e correlacionamento Monitoramento de estação detrabalho (Endpoint Detection and Response - EDR),
> Análise de Tráfego de Rede (Network Traffic Analysis - NTA),
> Análise de Comportamento de Usuário (User Entity and Behavior Analytics - UEBA),
> Análise de Inteligência de Ameaças Cibernéticas (Cyber Threat Intelligence - CTI) **E**
> de coleta Informações de segurança e gestão de eventos (Security Informati on and Event Management - SIEM) para um total de, no mínimo de;

3. Restitua-se o presente processo para continuidade do certame.

Atenciosamente,

Documento assinado eletronicamente por **IVANILDO DE OLIVEIRA DA SILVA JUNIOR**, **Integrante Requisitante**, em 03/03/2022, às 16:27, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **17359631** e o código CRC **3D290237**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

Referência: Processo nº 08006.000003/2021-38 SEI nº 17359631