

**A
TODAS AS LICITANTES,**

Ref.: Pregão Eletrônico nº 033/2022 - PROCESSO DAE nº 1597/2022

Esclarecimento

Objeto: Contratação de empresa especializada para prestar serviço de realização de testes de intrusão (Pentest) em redes, sistemas e ativos de tecnologia da informação e comunicação.

Prezados, Boa Tarde,

A STEFANINI RAFAEL SEGURANCA E DEFESA S.A, inscrita no CNPJ/MF sob o n.º 24.691.488/0001-09, com sede na Avenida Eusébio Matoso, 1375 – 8 Andar Sala 801 e 802, Butantã, São Paulo – SP, Cep: 05423-905, Brasil, vem, respeitosamente, à presença de Vossa Senhoria, solicitar **ESCLARECIMENTOS** aos **QUESTIONAMENTOS** em anexo, no que couber.

1- Para a perfeita precificação de serviços de testes de intrusão (Pentest), é imprescindível que o DAE Jundiaí, informe de maneira clara os quantitativos de testes e os tipos de testes que pretendem contratar (Black Box, Grey Box e White Box). Desta forma, referente ao Item 5 (Ambiente Computacional a Ser Analisado) do Anexo V – Termo de Referência, favor informar quais tipos de testes que o DAE Jundiaí pretende contratar para cada um dos ativo abaixo.

- 5.1. 6 IPs externos;
- 5.2. 4 aplicações WEB;
- 5.3. 1 aplicação Mobile;
- 5.4. 4 subdomínios;
- 5.5. 1 VPN
- 5.6. 59 servidores;
- 5.7. 417 estações de trabalho;
- 5.8. 90 dispositivos de rede;
- 5.9. 7 aplicações internas;
- 5.10. 1 rede sem fio;



2- Não é comum realizar testes de intrusão em ativos tipo estações de trabalho ou dispositivos de rede, nem mesmo em servidores a não ser que estes servidores contenham aplicações expostas na internet. Para estes tipos de ativos aplica-se comumente rastreamento de vulnerabilidades (Scan de Vulnerabilidades). Para os ativos abaixo, o DAE Jundiá pretende contratar Testes de Intrusão ou Rastreamento de Vulnerabilidades (Scan)?

- 5.6. 59 servidores;
- 5.7. 417 estações de trabalho;
- 5.8. 90 dispositivos de rede;

3- Para os ativos abaixo, favor informar quais são as aplicações, em qual ambiente de desenvolvimento foram criadas e qual plataforma de hardware estão instaladas.

a. 5.9. 7 aplicações internas;

4- O edital totaliza 590 testes de intrusão. Um teste do tipo Black Box (Teste mais simples), quando executado por um profissional sênior competente, utilizando ferramentas e processos tradicionais pode demorar até 40 horas (Dados de mercado). Um reteste tem a mesma duração do teste. O DAE Jundiá pretende executar todos estes 590 testes de intrusão e respectivos retestes em 90 dias?

Resposta:

1- R.: Todos Gray Box.

2- R: Rastreamento de Vulnerabilidades (Scan).

3- R: Como não há desenvolvimento de aplicações, o termo "Internas" é no sentido de não estarem disponíveis fora do ambiente computacional da DAE, apenas internamente, inclusive a instalação.

Aplicações:

- Sistema Comercial;
- Sistema de Recursos Humanos;
- ERP;
- Sistema de Geo;
- Sistema de Gestão de TI;
- Sistema de Laboratório;
- Gestão de Impressão.

A plataforma de desenvolvimento é de domínio dos fabricantes dos Softwares e não da DAE e a instalação compreende ambiente Windows e Linux.

4- R: O teste do ambiente deve durar 90 dias, porém está prevista a entrega de relatórios parciais. Dessa forma, a equipe da DAE poderá atuar na correção



das vulnerabilidades em paralelo com os testes, de maneira a minimizar o tempo do reteste.

Também é importante lembrar que o contrato vai além dos 90 dias, justamente para permitir a extensão do tempo do reteste, já que não há conhecimento prévio do que deverá ser feito.

Atenciosamente,

Anderson de Oliveira Faria
Pregoeiro/Seção de Compras e Licitações

Cassiano Marco Galzoni
Coordenador de TI (GTI)

