São Paulo, 21 de outubro de 2022.

CONCORRÊNCIA Nº 13713/2022
ABERTURA: DIA 27 DE OUTUBRO DE 2022 – ÀS 10H00
OBJETO: "SOLUÇÃO PARA TESTE DE SEGURANÇA DE APLICAÇÃO COM SERVIÇO DE IMPLEMENTAÇÃO E GERENCIAMENTO, CONSULTORIA EM GESTÃO DE RISCO DE SEGURANÇA DA INFORMAÇÃO E TREINAMENTOS".

CARTA DE ESCLARECIMENTOS I

Encaminhamos abaixo os questionamentos e as respostas a todos os participantes:

1) Cada um dos profissionais deverá ter qualquer uma das certificações indicadas, não sendo necessário que possua todas as certificações. Está correto o nosso entendimento?

RESPOSTA: Não, todos os profissionais deverão apresentar as certificações exigidas conforme edital.

2) Considerando que diversos dos itens dentre os subitens 9.20.1 a 9.20.10 não são certificações, mas sim áreas de conhecimento, conteúdos comuns a várias certificações, ou empresas fornecedoras de certificações, entendemos que não é necessário atender a todos os subitens 9.20.1 a 9.20.10, mas apenas que os profissionais alocados possuam alguma das certificações indicadas (ou das empresas indicadas). Está correto esse entendimento?

RESPOSTA: A equipe de profissionais deve apresentar todas as certificações exigidas conforme edital.

3) 9.20.2 GDPR / LGPD certification - Será aceita qualquer certificação em LGPD ou GDPR. Está correto esse entendimento?

RESPOSTA: Será aceita toda certificação correspondente a LGPD ou GDPR.

4) 9.20.4 Information Security Risk Management - Trata-se de uma área de conhecimento. Será aceita qualquer certificação na área de segurança da informação que possua gestão de riscos em seu conteúdo, como, por exemplo, a Security+. Está correto esse entendimento?

RESPOSTA: Será aceita toda certificação que trate exclusivamente de Gestão de Risco de Segurança da Informação.

5) 9.20.5 Certified Threat Intelligence Analyst - Duas certificações foram identificadas com esse nome. A CTIA da National Initiative for Cybersecurity Careers and Studies (https://niccs.cisa.gov/education-training/catalog/justone-solutions-llc/certified-threat-intelligence-analyst-ctia), e da EC-Council (https://www.eccouncil.org/programs/threat-intelligence-training/). Além disso, outras certificações tratam do assunto. Será aceita qualquer certificação na área de threat intelligence. Está correto esse entendimento?

RESPOSTA: Ambas as certificações serão aceitas.

6) 9.20.6 eLearnSecurity - eLearnSecurity fornece diversas certificações na área de cibersegurança. Será aceita qualquer certificação da eLearnSecurity. Está correto esse entendimento?

RESPOSTA: Todas as certificações de Segurança da Informação da eLeanSecurity serão aceitas.

7) 9.20.7 eCPPT (eLearnSecurity Certified Professional Penetration Tester) - eCPPT é uma das certificações profissionais fornecidas pela eLearnSecurity, certificando a capacidade profissional de "Penetration Testers". Considerando o art. 7o §5o da lei de licitações ("É vedada a realização de licitação cujo objeto inclua bens e serviços sem similaridade ou de marcas, características e especificações exclusivas"). Considerando que há outras certificações que certificam capacidades profissionais similares, entendemos que certificações profissionais bem reconhecidas da mesma área e nível, ou de nível mais avançado, também serão aceitas. Como exemplo de atendimento de requisito por similaridade de características citamos a OSCP. Está correto esse entendimento?

RESPOSTA: Entendemos que a certificação OSCP seja compatível com item exigido em nosso edital.

8) 9.20.8 Advanced Memory Forensics and Threat Detection - Análise forense de memória e detecção de ameaças são conteúdos comuns a diferentes cursos de ciber-segurança, principalmente nas áreas de forense e de resposta a incidentes. Não identificamos nenhuma certificação específica com esse nome ou somente com esse conteúdo. No passado o instituto SANS possuía um "bootcamp" exatamente com esse nome (que não está mais disponível). Bootcamps possuem certificado de participação, o que é diferente de uma certificação profissional. Entendemos que será aceita qualquer certificação

profissional que tenha em seus conteúdos a análise de memória e detecção de ameaças. Está correto esse entendimento?

RESPOSTA: Aceitaremos toda certificação que ateste competência em análise de memória e detecção de ameaça.

9) 9.20.9 Buffer Overflow Windows e Linux - Buffer overflows em windows e linux são conteúdos comuns a diferentes cursos e certificações de cibersegurança, principalmente na área de testes de invasão. Não identificamos nenhuma certificação específica com esse nome ou somente com esse conteúdo. Entendemos que será aceita qualquer certificação profissional que tenha em seus conteúdos a execução de buffer overflows. Está correto esse entendimento?

RESPOSTA: Aceitaremos toda certificação que ateste conhecimentos em buffer overflow.

10) Qual a quantidade de aplicações envolvidas neste escopo.

RESPOSTA: 480 Aplicações

11) Quantas destas aplicações são microserviços?

RESPOSTA: Todas as Aplicações são microserviços

12) "Linguagens utilizadas: Exemplo: Java, .Net, C++, NodeJS, Python, etc"

RESPOSTA: Java, .NET, Coldfusion, C# e NodeJs

13) "Repositório de código: Exemplo: Github, Gitlab, Git on-premise, etc"

RESPOSTA: GitLab

14) "CI/CD utilizados para executar o pipeline: Exemplo: Jenkins, Gitlab, Azure DevOps, Bitrise, AWS, etc"

RESPOSTA: Jenkins

15) "Controle de bugs (bug/defect tracking) utilizados: Exemplo: Jira, Azure Boards/DevOps, Bugzilla, etc"

RESPOSTA: Não é utilizado

16) "IDE's utilizadas: Exemplo: Eclipse, Visual Studio, VSCode, IntelliJ, etc"

RESPOSTA: Eclipse, VSCode, Sublime e Visual Studio

17) Qual a quantidade de desenvolvedores?

RESPOSTA: 60 desenvolvedores

18) Quais domínios e subdomínios serão monitorados?

RESPOSTA: Os domínios por questões de segurança não podem ser disponibilizados e a contratado deverá inventariar.
Quantidade - 2 domínios.

19) Quantas e quais nuvens estarão envolvidas no escopo para avaliação de vulnerabilidades/conformidades?

RESPOSTA: Cloud (Nuvem) do tipo Plataforma Azure-Microsoft entre outras passiveis de integração.

20) Para a gestão de vulnerabilidade de infra qual a quantidade de IPs estão envolvidos neste escopo?

RESPOSTA: Mesma quantidade de aplicações disponibilizadas e envolvidas no escopo.

COMISSÃO PERMANENTE DE LICITAÇÃO