Respostas aos questionamentos (2)

Licitação 029/2021

Contratação de Serviços de Consultoria para Diagnóstico, a fim de adequar a NUCLEP ao disposto na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

Av. Gal. Euclydes de Oliveira Figueiredo, 200 - Brisamar - Itaguaí – RJ, Cep: 23825-410
+55 21 3781-4500 | www.nuclep.gov.br | secretaria.adm@nuclep.gov.br

Empresa:
EY

Contato:
Patricia Paiva, por e-mail em 20/05/2021

Questões:

1 - Qual a quantidade de colaboradores da empresa?

Resposta 1:
Cerca de 800 colaboradores

2- Quantidade de departamentos na empresa?

Resposta 2:
3 Diretorias, 10 Gerências Gerais e 50 Gerências

3 - Quantos processos de negócio em média existem em cada departamento (estimativa)?

Resposta 3:
Número desconhecido. Será feito levantamento sob responsabilidade da consultoria com apoio da Nuclep. A descrição dos processos será sucinta, sem necessidade de detalhamentos.

4 - A empresa possui Gerente de Segurança da Informação (SI), ou outro Gestor responsável pela SI da empresa?

Resposta 4:
A gestão da Segurança da Informação é feita pela Gerência Geral de Tecnologia da Informação em conjunto com o Comitê Gestor de Segurança da Informação (CGSI).

5 - Item 4.1.7 - Pelo momento de pandemia que estamos vivendo, podemos entender que preferencialmente podemos considerar o trabalho sendo executado de forma remota?

Resposta 5:
Não. A preferência será pelo trabalho presencial. Seguindo os termos apresentados no TR, por conveniência e sob autorização expressa da Nuclep, em comum acordo, algumas atividades poderão eventualmente ser executadas remotamente, mas devem ser consideradas e precificadas como atividades inteiramente presenciais.

6 - Qual é o número total de aplicações no escopo do teste de invasão?

Resposta 6:
Cerca de 40 aplicações.

7 - Qual é o tipo de abordagem desejada para os testes (Black, Gray, White) ?

Resposta 7:
Não entramos em detalhes na abordagem no TR. Sugerimos a aplicação progressiva das abordagens entre Black box, Gray Box e um relatório final em White Box. Seria o modo mais custoso, mas certamente o mais seguro e mais completo para apresentar um amplo teste de intrusão. (Na eventualidade de decidirmos por uma abordagem, recomendamos gray box que balanceia as demais abordagens)

8 - Os testes podem ser executados remotamente ?

Resposta 8:
Alguns testes poderão ser feitos remotamente, mas uma análise local do ambiente é imprescindível para dar uma visão mais abrangente de eventuais ameaças internas.

9 - Qual a quantidade de aplicações legadas ?

Resposta 9:
Pelo menos 5 aplicações são legadas.

10 - Engenharia Social faz parte do escopo de testes?

Resposta 10:
É desejável fazer parte do escopo de teste, mas não entramos em detalhes sobre a metodologia. Gostaríamos que fosse o mais abrangente possível.

11 - Qual a quantidade de APIs?

Resposta 11:
Não possuímos esta informação quantificada.

12 - Qual é o número total de endpoints monitorados ?

Resposta 12:
Aproximadamente 800 computadores. Mais de 90% com Windows 10.

13 - Qual é o número total de servidores monitorados?

Resposta 13:
São 7 servidores físicos e 55 servidores virtuais.

14 - Ambientes OT, Automação, Fabril e IOT fazem parte do escopo?

Resposta 14:
As estações fabris não operam dentro da nossa rede corporativa, utilizando-se de rede segregada ou ainda isoladas da rede. Contamos com cerca de vinte desses equipamentos para automação no parque industrial em funções variadas. Nesse sentido, fazem parte do escopo da análise, porém acreditamos que não contenham dados pessoais armazenados ou tratados nas mesmas.

15 - Qual é a proporção da distribuição do deployment em cloud ? % Azure, % AWS, % Outros.

Resposta 15:
Não contamos com solução cloud da Azure e AWS. Utilizamos apenas serviços de hospedagem de website e e-mail, ambos hospedados e administrados em data center externo.

16 - Quantidade de usuários?

Resposta 16:
Cerca de 800 usuários.

17 - Quantos servidores estão instalados no ambiente On Premisse ?

Resposta 17:
Atualmente, 2 virtualizadores em produção, 1 Storage em produção, 1 Servidor de Backup em produção. Há iniciativas em andamento para incrementos de disponibilidade com replicação de ambiente e serviços, mas ainda não está concluída. Em 60 dias temos a expectativa de estarmos com 3 virtualizadores, 2 storages e 2 servidores de backup no site fabril.

19 - Qual é a ferramenta de AV utilizada ?

Resposta 19:
Kaspersky Endpoint Security

20 - Quantos sites são monitorados ?

Resposta 20:
Na prática temos um único site. Há um escritório no centro do Rio de Janeiro com apenas 2 colaboradores fixos e outras 6 estações de trabalho básicas para uso eventual em reuniões e visitas.

21 - Existe uma solução de SOC ?

Resposta 21:
Não

22 - Qual é a ferramenta de SIEM utilizada ?

Resposta 22:
Não dispomos de ferramenta de SIEM.

23 – Entendemos que a equipe técnica e suas devidas comprovações exigidas no item 7.2 do Termo de Referência, deverão ser comprovados no momento da contratação. Sendo assim, para fins de habilitação técnica, será necessário apresentar na licitação apenas o atestado de capacidade técnica da empresa (item 11.2 do Edital). Nosso entendimento está correto?

Resposta 23:
Conforme TR, o entendimento está correto, sob pena de desclassificação no momento da contratação, no caso de não atendimento às premissas necessárias.

24 – Ainda sobre a equipe técnica exigida no item 7.2 do Termo de Referência, gostaríamos de esclarecer como deverá ser comprovada a experiência da equipe de acordo com cada perfil.

Resposta 24:
Através de Atestados de Capacitação Técnica emitidos por responsáveis das organizações públicas ou privadas na qual estes profissionais atuaram.

Helio Araujo e Castro
Assinado de forma digital por Helio Araujo e Castro
Dados: 2021.05.27 14:41:16 -03'00'