CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

ESCLARECIMENTOS Nº 5

Pregão Eletrônico nº 12/2024 (90.012/2024)

Considerando os questionamentos recebidos a respeito da licitação em referência, o Coren-SP torna público:

QUESTIONAMENTO 1

Qual o prazo para concluir os testes de intrusão e análise de vulnerabilidades?

Resposta da Equipe de Planejamento da Contratação - EPC:

Conforme prevê o item 4.9 do Anexo I; itens 2.27 e 3.1.18 do Anexo II; entre outros.

QUESTIONAMENTO 2

Quais ferramentas o Coren-SP usa para análise de vulnerabilidades e pentest?

Resposta da Equipe de Planejamento da Contratação - EPC:

Nenhuma ferramenta atualmente. O presente objeto trata exatamente de endereçar essa questão, através de fornecimento em forma de serviço.

QUESTIONAMENTO 3

O Coren-SP exige presença física da equipe ou os testes podem ser feitos remotamente?

Resposta da Equipe de Planejamento da Contratação - EPC:

No decorrer do Edital e Anexos foram detalhados pontos referentes a necessidade de atuação remota e presencial, a depender do serviço. Serviços de Pentest e Análise de Vulnerabilidades podem ser executados remotamente. Já os serviços de Engenharia Social os quais sejam detalhados no item 3.2.4 do Anexo II precisam, por uma questão conceitual, ser executados de forma presencial.

QUESTIONAMENTO 4

Qual o plano para tratar vulnerabilidades críticas identificadas durante os testes?

Resposta da Equipe de Planejamento da Contratação - EPC:

Priorizar a correção de vulnerabilidades críticas com engajamento das equipes responsáveis conforme o alvo da vulnerabilidade encontrada.

QUESTIONAMENTO 5

Quantas horas são necessárias para elaborar relatórios e retestes após correções?

Resposta da Equipe de Planejamento da Contratação - EPC:

Conforme prevê o item 4.9 do Anexo I; itens 2.27 e 3.1.18 do Anexo II; entre outros.

QUESTIONAMENTO 6

Como o Coren-SP quer distribuir as horas entre pentest, análise de vulnerabilidades e engenharia social?

Resposta da Equipe de Planejamento da Contratação - EPC:
Conforme prevê os itens 1.7 e 3.1.2 do Anexo II.

QUESTIONAMENTO 7
O Coren-SP requer treinamento para a equipe interna após a entrega dos relatórios?

Resposta da Equipe de Planejamento da Contratação - EPC:
A contratada deve disponibilizar treinamento em vídeo, palestra ou treinamento online para conscientização de todos os usuários, sobre os temas testados, ao final da campanha, conforme previsto no item 3.2.12 do Anexo II.

QUESTIONAMENTO 8
Como o Coren-SP garante a confidencialidade e sigilo das informações durante os testes?

Resposta da Equipe de Planejamento da Contratação - EPC:
Essa garantia deve ser oferecida pela contratada.

QUESTIONAMENTO 9
Quais certificações são exigidas para validar os relatórios?

Resposta da Equipe de Planejamento da Contratação - EPC:
As certificações estão previstas no item 1.6 do Anexo II.

QUESTIONAMENTO 10
Quantas rodadas de reteste estão incluídas no contrato?

Resposta da Equipe de Planejamento da Contratação - EPC:
Conforme previsto nos Itens 1.8.3 e 3.1.18 do Anexo II.

QUESTIONAMENTO 11
Quais métricas o Coren-SP usará para avaliar a eficácia dos testes?

Resposta da Equipe de Planejamento da Contratação - EPC:
Conforme item 2.1 do Anexo II, a Contratada deve excluir falso-positivos do relatório, garantindo assim a eficácia dos testes.

QUESTIONAMENTO 12
O serviço inclui a criação de um plano de ação para mitigação de vulnerabilidades?

Resposta da Equipe de Planejamento da Contratação - EPC:
Solicitamos observar os itens 2.35.13 e 3.1.1 do Anexo II.

QUESTIONAMENTO 13
Há restrições de acesso a sistemas ou dispositivos durante os testes?

Resposta da Equipe de Planejamento da Contratação - EPC:

Conforme disposto no item 2.9 do Anexo II, "A contratada deve dispor de todos os recursos para a realização das análises e testes, ficando o Coren-SP obrigado apenas a providenciar acesso a infraestrutura para realização dos preparativos e dos testes propriamente ditos.".

QUESTIONAMENTO 14

Haverá necessidade de treinamento adicional para a equipe do Coren-SP? Qual o escopo?

Resposta da Equipe de Planejamento da Contratação - EPC:

A contratada deve disponibilizar treinamento em vídeo, palestra ou treinamento online para conscientização de todos os usuários, sobre os temas testados, ao final da campanha, conforme previsto no item 3.2.12 do Anexo II.

QUESTIONAMENTO 15

Qual a frequência recomendada para análises de vulnerabilidades durante o contrato?

Resposta da Equipe de Planejamento da Contratação - EPC:

Conforme previsto nos Itens 1.8.3 e 3.1.18 do Anexo II.

QUESTIONAMENTO 16

Como integrar as ferramentas de pentest aos sistemas de segurança existentes no Coren-SP?

Resposta da Equipe de Planejamento da Contratação - EPC:

As ferramentas de pentest devem ser capazes de fazer análises e testes de intrusão independentemente do ambiente. Apesar disso e para melhor compreensão do ambiente do Coren-SP, há informações sobre o ambiente da contratante nos itens 1.7 e 1.8 do Anexo II.

QUESTIONAMENTO 17

Os relatórios devem incluir análise comparativa com benchmarks do setor? Quais?

Resposta da Equipe de Planejamento da Contratação - EPC:

Conforme disposto nos itens 3.2.14 e 3.2.20 do Anexo II.

QUESTIONAMENTO 18

Como o Coren-SP deseja que sejam tratados o armazenamento e a segurança das credenciais e dados sensíveis?

Resposta da Equipe de Planejamento da Contratação - EPC:

Conforme padrões e boas práticas de mercado.

QUESTIONAMENTO 19

Quais vulnerabilidades o Coren-SP quer verificar com base em OWASP e NIST?

Resposta da Equipe de Planejamento da Contratação - EPC:

Todas as quais sejam aplicáveis ao ambiente do Coren-SP, conforme descrito nos itens 1.3, 2.32, 3.1.8, 3.1.9, 3.1.27 e 3.1.29.7 do Anexo II.

QUESTIONAMENTO 20

Como evitar falsos positivos na análise de vulnerabilidades?

Resposta da Equipe de Planejamento da Contratação - EPC:

Entendemos que esse conhecimento é parte da entrega do serviço a ser contratado e que, portanto, deve fazer parte do know-how da empresa contratada.

QUESTIONAMENTO 21

O Coren-SP deseja relatórios intermediários antes da entrega final? Com que frequência?

Resposta da Equipe de Planejamento da Contratação - EPC:

Não incluído em Edital, logo não se aplica à referida contratação.

QUESTIONAMENTO 22

Qual metodologia o Coren-SP recomenda para minimizar o impacto nos sistemas durante os testes?

Resposta da Equipe de Planejamento da Contratação - EPC:

Entendemos que esse conhecimento é parte da entrega do serviço a ser contratado e que, portanto, deve fazer parte do know-how da empresa contratada.

QUESTIONAMENTO 23

O Coren-SP requer testes em dispositivos móveis ou apenas em infraestrutura de rede e servidores?

Resposta da Equipe de Planejamento da Contratação - EPC:

Solicitamos observar o disposto no item 1.8.3 do anexo II.

QUESTIONAMENTO 24

Os resultados das campanhas de phishing devem incluir métricas sobre o comportamento dos usuários? Quais?

Resposta da Equipe de Planejamento da Contratação - EPC:

Conforme disposto nos itens 3.2.14 e 3.2.20 do Anexo II.

QUESTIONAMENTO 25

O Coren-SP deseja testes de stress ou simulações de ataque prolongado? Quais objetivos?

Resposta da Equipe de Planejamento da Contratação - EPC:

Não incluído em Edital, logo não se aplica à referida contratação.

QUESTIONAMENTO 26

Quais desafios específicos o Coren-SP espera durante os testes?

Resposta da Equipe de Planejamento da Contratação - EPC:

Ainda não temos o serviço em questão no Coren-SP. Portanto, essa questão será tratada na reunião inicial com o fornecedor.

QUESTIONAMENTO 27

Como o Coren-SP integrará a gestão de logs ao processo de auditoria e análise?

Resposta da Equipe de Planejamento da Contratação - EPC:

Entendemos que essa tarefa/responsabilidade pertence a contratada e não ao Coren-SP.

QUESTIONAMENTO 28

Como o Coren-SP lidará com a exclusão ou anonimização de dados pessoais sensíveis ao final dos testes?

Resposta da Equipe de Planejamento da Contratação - EPC:

Entendemos que essa tarefa/responsabilidade pertence a contratada e não ao Coren-SP.

QUESTIONAMENTO 29

Quais práticas de gerenciamento de riscos o Coren-SP adota para testes de segurança?

Resposta da Equipe de Planejamento da Contratação - EPC:

Ainda não temos esse serviço/processo implementado. Portanto, o objeto em questão será importante para a definição de práticas e procedimentos.

QUESTIONAMENTO 30

O Coren-SP tem um plano para atualizar continuamente ferramentas e metodologias usadas?

Resposta da Equipe de Planejamento da Contratação - EPC:

Entendemos que essa tarefa/responsabilidade pertence a contratada e não ao Coren-SP.

QUESTIONAMENTO 31

Como o Coren-SP deseja documentar e comunicar descobertas de vulnerabilidades?

Resposta da Equipe de Planejamento da Contratação - EPC:

Ainda não temos esse serviço/processo implementado. Portanto, o objeto em questão será importante para a definição de práticas e procedimentos.

QUESTIONAMENTO 32

Qual o nível de detalhamento esperado nos relatórios de vulnerabilidades e recomendações?

Resposta da Equipe de Planejamento da Contratação - EPC:

Deve seguir padrões de mercado especificados no Edital e Anexos, a exemplo do item 6.1.2 do Anexo I.

QUESTIONAMENTO 33

O Coren-SP requer testes de segurança em APIs? Quais?

Resposta da Equipe de Planejamento da Contratação - EPC:

Solicitamos observar o disposto no item 3.1.6 do Anexo II.

QUESTIONAMENTO 34

Como avaliar o impacto dos testes na performance dos sistemas?

Resposta da Equipe de Planejamento da Contratação - EPC:

Entendemos que esse conhecimento é parte da entrega do serviço a ser contratado e que, portanto, deve fazer parte do know-how da empresa contratada.

QUESTIONAMENTO 35

O Coren-SP deseja análise de configurações de segurança em sistemas operacionais e aplicativos? Quais?

Resposta da Equipe de Planejamento da Contratação - EPC:

Solicitamos observar o disposto no item 2.30.6 do Anexo II.

QUESTIONAMENTO 36

Como tratar dependências externas e integrações de terceiros durante os testes?

Resposta da Equipe de Planejamento da Contratação - EPC:

Entendemos que esse conhecimento é parte da entrega do serviço a ser contratado e que, portanto, deve fazer parte do know-how da empresa contratada.

QUESTIONAMENTO 37

Qual é o processo para validar correções após a identificação de vulnerabilidades?

Resposta da Equipe de Planejamento da Contratação - EPC:

Conforme disposto no item 3.1.18 do Anexo II, trata-se de reteste.

QUESTIONAMENTO 38

Como gerenciar falhas de comunicação ou desacordo durante o projeto?

Resposta da Equipe de Planejamento da Contratação - EPC:

Entendemos que esse conhecimento é parte da entrega do serviço a ser contratado e que, portanto, deve fazer parte do know-how da empresa contratada.

QUESTIONAMENTO 39

Quais estratégias usar para simular cenários reais de ataques?

Resposta da Equipe de Planejamento da Contratação - EPC:

Entendemos que esse conhecimento é parte da entrega do serviço a ser contratado e que, portanto, deve fazer parte do know-how da empresa contratada.

QUESTIONAMENTO 40

Como abordar questões de compliance e regulatórias durante os testes?

Resposta da Equipe de Planejamento da Contratação - EPC:

Entendemos que esse conhecimento é parte da entrega do serviço a ser contratado e que, portanto, deve fazer parte do know-how da empresa contratada.

QUESTIONAMENTO 41

O Coren-SP requer análise de segurança em ambientes de nuvem? Quais?

Resposta da Equipe de Planejamento da Contratação - EPC:

Conforme disposto no item 3.1.6 do Anexo II.

QUESTIONAMENTO 42

Como garantir a eficácia das estratégias de engenharia social aplicadas?

Resposta da Equipe de Planejamento da Contratação - EPC:

Entendemos que esse conhecimento é parte da entrega do serviço a ser contratado e que, portanto, deve fazer parte do know-how da empresa contratada.

QUESTIONAMENTO 43

Qual a metodologia para avaliar a segurança física e controles de acesso?

Resposta da Equipe de Planejamento da Contratação - EPC:

Entendemos que esse conhecimento é parte da entrega do serviço a ser contratado e que, portanto, deve fazer parte do know-how da empresa contratada.

QUESTIONAMENTO 44

Como priorizar vulnerabilidades para correção?

Resposta da Equipe de Planejamento da Contratação - EPC:

Conforme disposto no item 3.1.13 do Anexo II.

QUESTIONAMENTO 45

Quais medidas tomar para mitigar impactos durante os testes de segurança?

Resposta da Equipe de Planejamento da Contratação - EPC:

Entendemos que esse conhecimento é parte da entrega do serviço a ser contratado e que, portanto, deve fazer parte do know-how da empresa contratada.

QUESTIONAMENTO 46

Haverá revisão pós-testes para avaliar as ações corretivas? Como?

Resposta da Equipe de Planejamento da Contratação - EPC:

Conforme disposto no item 3.1.18 do Anexo II, trata-se de reteste.

UESTIONAMENTO 47

Como garantir a precisão dos dados coletados durante os testes?

Resposta da Equipe de Planejamento da Contratação - EPC:

Entendemos que esse conhecimento é parte da entrega do serviço a ser contratado e que, portanto, deve fazer parte do know-how da empresa contratada.

QUESTIONAMENTO 48

Qual o plano para atualizar políticas de segurança com base nos resultados dos testes?

Resposta da Equipe de Planejamento da Contratação - EPC:

Ainda não temos esse serviço/processo implementado. Portanto, o objeto em questão será importante para a definição de práticas e procedimentos.

QUESTIONAMENTO 49

Como acompanhar as recomendações de segurança após a entrega dos relatórios?

Resposta da Equipe de Planejamento da Contratação - EPC:

Conforme disposto no item 3.1.18 do Anexo II, trata-se de reteste.

QUESTIONAMENTO 50

Qual abordagem para validar os resultados e feedback após os testes?

Resposta da Equipe de Planejamento da Contratação - EPC:

Conforme disposto no item 3.1.18 do Anexo II, trata-se de reteste.

São Paulo, 15 de setembro de 2024.

Rachel Konno Serra

Assinado de forma digital por Rachel Konno Serra
Dados: 2024.09.15 13:48:42 -03'00'

Rachel Konno Serra
Pregoeira

Publicado no site do Coren-SP https://portal.coren-sp.gov.br/licitacoes/pregao-eletronico-no-12-2024-90012-2024-analise-de-vulnerabilidades/ *e no portal: www.gov.br/compras/*