MINISTÉRIO DO PLANEJAMENTO E ORÇAMENTO
SECRETARIA DE ORÇAMENTO FEDERAL
SUBSECRETARIA DE TECNOLOGIA E DESENVOLVIMENTO INSTITUCIONAL

CARGO 8: ANALISTA DE PLANEJAMENTO E ORÇAMENTO – ESPECIALIDADE: GESTÃO DA SEGURANÇA DA INFORMAÇÃO ORÇAMENTÁRIA

Prova Discursiva P_4 – Dissertação

Aplicação: 07/07/2024

PADRÃO DE RESPOSTA DEFINITIVO

1. **Vantagens da criptografia simétrica**: adequada para uso de grande quantidade de dados; implementação e uso simplificado; demanda menos tempo de processamento.
   Desvantagens: uso da mesma chave tanto para criptografar como para descriptografar os dados; impossibilidade de identificação da identidade de quem a enviou ou de quem a recebeu; não permite a usabilidade de assinatura digital.

2. **Vantagens da criptografia assimétrica**: garantia da confidencialidade e autenticação das informações entre duas partes; alta taxa de segurança; autenticação das informações através da assinatura digital.
   Desvantagens: utilização de mais recursos computacionais; mais complexa de implementar e usar; mais lenta que a criptografia simétrica; o texto cifrado é maior que o texto original ou do mesmo tamanho; é mais cara que a simétrica.

3. **Segmentos de atividades do Blue Team**: segurança defensiva; proteção de infraestrutura; controle de danos; respostas a incidentes; segurança operacional; identificação de ameaças; forense digital.
   Segmentos de atividades do Red Team: segurança ofensiva; *ethical hacking*; análise de vulnerabilidades; testes de intrusão; engenharia social.

4. **Objetivo dos controles criptográficos, segundo a norma ABNT NBR ISO/IEC 27001**: assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, a autenticidade e(ou) a integridade da informação.

5. **Fases em que se subdivide a análise de risco, segundo a norma ABNT NBR ISO/IEC 27005**: a análise de riscos é uma fase do processo que é subdividida em três fases: identificação dos riscos, análise de riscos e avaliação de riscos.

6. **Riscos de segurança de aplicativos da Web, de acordo com o *framework* OWASP Top Ten de 2021**: controle de acesso quebrado; falhas criptográficas; injeção; *design* inseguro; configuração incorreta de segurança; componentes vulneráveis e desatualizados; falhas de identificação e autenticação; falhas de integridade de *software* e dados; falhas de registro e monitoramento de segurança; SSRF (*server-side request forgery*).

7. **Resposta a incidentes de segurança da informação**: segundo o CERT.br, a resposta a incidentes de segurança é uma metodologia organizada para gerir consequências de uma violação de segurança de informação, ou seja, um planejamento de atuação contra qualquer tipo de evento que coloque em risco os sistemas de informação. Pode-se dizer que Resposta a incidentes é o processo que descreve como uma organização deverá lidar com um incidente de segurança.

8. **Serviços providos pelo CTIR Gov**: o conjunto desses serviços pode ser dividido em notificação de incidentes; análise de incidentes; suporte à resposta a incidentes; coordenação na resposta a incidentes; distribuição de alertas, recomendações e estatísticas; e cooperação com outras equipes de tratamento de incidentes.
   Referência: https://www.gov.br/ctir/pt-br/assuntos/servicos

9. **Etapas principais da computação forense**: coleta, exame, análise e relatório. O objetivo da primeira etapa é identificar, isolar, etiquetar, registrar e coletar os dados e evidências físicas relacionadas com o incidente que está sendo investigado, enquanto estabelece e mantém a integridade das provas. No exame: identificar e extrair as informações relevantes a partir dos dados coletados utilizando ferramentas e técnicas forenses adequadas. Na análise, o objetivo é analisar os resultados do exame para gerar respostas úteis para as questões apresentadas nas fases anteriores. Em relatório (resultados), inclui

encontrar relevância para o caso, sendo redigido o laudo pericial, o qual deve ter conclusão imparcial, clara e concisa.
Fonte: KENT, K. et al. Guide to integrating forensic techniques into incident response: Special publication. Gaithersburg: NIST, 2006.

QUESITOS AVALIADOS

QUESITO 2.1 Uma vantagem e uma desvantagem de criptografia simétrica
Conceito 0 – Não atendeu ao solicitado ou o fez de forma totalmente equivocada.
Conceito 1 – Discorreu corretamente apenas sobre uma vantagem ou uma desvantagem.
Conceito 2 – Discorreu, de forma parcialmente correta ou insuficiente sobre uma vantagem e uma desvantagem.
Conceito 3 – Discorreu correta e suficientemente sobre uma vantagem e uma desvantagem.

QUESITO 2.2 Uma vantagem e uma desvantagem de criptografia assimétrica
Conceito 0 – Não atendeu ao solicitado ou o fez de forma totalmente equivocada.
Conceito 1 – Discorreu corretamente apenas sobre uma vantagem ou uma desvantagem.
Conceito 2 – Discorreu, de forma parcialmente correta ou insuficiente, sobre uma vantagem e uma desvantagem.
Conceito 3 – Discorreu correta e suficientemente sobre uma vantagem e uma desvantagem.

QUESITO 2.3 Um segmento de atividade do Blue Team e um segmento de atividade do Red Team na defesa de ataques cibernéticos
Conceito 0 – Não atendeu ao solicitado ou o fez de forma totalmente equivocada.
Conceito 1 – Citou corretamente apenas um segmento do Blue Team ou um do Red Team.
Conceito 2 – Citou corretamente um segmento de cada um dos times.

QUESITO 2.4 Objetivo dos controles criptográficos em relação ao gerenciamento de segurança da informação, segundo a norma ABNT NBR ISO/IEC 27001
Conceito 0 – Não atendeu ao solicitado ou o fez de forma totalmente equivocada.
Conceito 1 – Explicou o objetivo de forma parcialmente correta ou insuficiente.
Conceito 2 – Explicou de forma correta e completa o objetivo.

QUESITOS 2.5 As três fases em que se subdivide a análise de riscos, conforme a norma NBR ISO/IEC 27005
Conceito 0 – Não atendeu ao solicitado ou o fez de forma totalmente equivocada.
Conceito 1 – Citou corretamente apenas uma fase.
Conceito 2 – Citou corretamente apenas duas fases.
Conceito 3 – Citou corretamente as três fases.

QUESITO 2.6 Três riscos de segurança de aplicativos da Web, de acordo com o *framework* OWASP Top Ten de 2021
Conceito 0 – Não atendeu ao solicitado ou o fez de forma totalmente equivocada.
Conceito 1 – Exemplificou corretamente apenas um risco.
Conceito 2 – Exemplificou corretamente apenas dois riscos.
Conceito 3 – Exemplificou corretamente três riscos.

QUESITO 2.7 Resposta a incidentes de segurança da informação
Conceito 0 – Não atendeu ao solicitado ou o fez de forma totalmente equivocada.
Conceito 1 – Explicou de forma apenas superficial o conceito de resposta a incidentes de segurança da informação.
Conceito 2 – Explicou o conceito de forma parcialmente correta ou insuficiente.
Conceito 3 – Explicou o conceito de forma correta e suficiente.

QUESITO 2.8 Quatro serviços providos pelo CTIR Gov
Conceito 0 – Não atendeu ao solicitado ou o fez de forma totalmente equivocada.
Conceito 1 – Citou corretamente apenas um serviço.
Conceito 2 – Citou corretamente apenas dois serviços.
Conceito 3 – Citou corretamente apenas três serviços.
Conceito 4 – Citou corretamente quatro serviços.

QUESITO 2.9 Duas das principais etapas de uma investigação forense e um objetivo de cada uma delas
Conceito 0 – Não atendeu ao solicitado ou o fez de forma totalmente equivocada.
Conceito 1 – Citou corretamente apenas uma etapa e não mencionou o respectivo objetivo ou mencionou o objetivo errado.
Conceito 2 – Citou corretamente apenas uma etapa com o respectivo objetivo.
Conceito 3 – Citou corretamente duas etapas, mas errou um dos objetivos.
Conceito 4 – Citou corretamente duas etapas com os respectivos objetivos.

Cebraspe
Centro Brasileiro de Pesquisa em Avaliação e Seleção e de Promoção de Eventos

MINISTÉRIO DO PLANEJAMENTO E ORÇAMENTO
SECRETARIA DE ORÇAMENTO FEDERAL
SUBSECRETARIA DE TECNOLOGIA E DESENVOLVIMENTO INSTITUCIONAL

CARGO 8: ANALISTA DE PLANEJAMENTO E ORÇAMENTO – ESPECIALIDADE: GESTÃO DE SEGURANÇA DA INFORMAÇÃO ORÇAMENTÁRIA

Prova Discursiva P_4 – Questão

Aplicação: 07/07/2024

PADRÃO DE RESPOSTA DEFINITIVO

O modelo de fundação assemelha-se a uma grande enciclopédia digital que foi lida e compreendida por uma inteligência artificial. Esses modelos são treinados com uma quantidade enorme de dados, abrangendo uma variedade de tópicos muito grande. Eles aprendem padrões e informações gerais que podem ser aplicados a uma ampla gama de tarefas sem a necessidade de grandes ajustes. Isso os torna extremamente flexíveis e poderosos, capazes de entender e gerar linguagem, resolver problemas e até criar arte de modo semelhante ao trabalho humano.

RAG (*retrieval-augmented generation*) é como um assistente inteligente que, ao receber uma pergunta, rapidamente consulta uma biblioteca imensa para buscar a informação mais relevante antes de responder. Ele combina a capacidade de geração de respostas do modelo de fundação com um mecanismo de busca, trazendo informações precisas e atualizadas. Isso é particularmente útil em tarefas que exigem respostas detalhadas e baseadas em evidências, como responder perguntas complexas ou fornecer recomendações detalhadas.

O modelo de fundação customizado é uma adaptação mais personalizada desses grandes modelos enciclopédicos. Caso uma empresa tenha necessidades muito específicas, como entender jargões técnicos de uma área específica como engenharia, tecnologia da informação, medicina, direito, entre outras áreas, ou responder a perguntas sobre leis de patentes, um modelo de fundação customizado pode ser ajustado para se especializar nesses tópicos, proporcionando resultados mais precisos e relevantes para a empresa. Ele é customizado para absorver e refletir o conhecimento e as necessidades específicas de seu treinamento, oferecendo uma ferramenta poderosa e personalizada para tarefas específicas.

Esses modelos não são apenas ferramentas, sendo também considerados recursos de busca contínua para expansão das capacidades humanas por meio da tecnologia.

QUESITOS AVALIADOS

QUESITO 2.1
Conceito 0 – Não abordou o quesito ou o fez de forma totalmente equivocada.
Conceito 1 – Descreveu o modelo de forma apenas superficial, sem desenvolvimento.
Conceito 2 – Desenvolveu uma descrição do modelo de forma parcialmente correta ou insuficiente.
Conceito 3 – Desenvolveu uma descrição do modelo de forma correta e completa.

QUESITO 2.2
Conceito 0 – Não abordou o quesito ou o fez de forma totalmente equivocada.
Conceito 1 – Descreveu o modelo de forma apenas superficial, sem desenvolvimento.
Conceito 2 – Desenvolveu uma descrição do modelo de forma parcialmente correta ou insuficiente.
Conceito 3 – Desenvolveu uma descrição do modelo de forma correta e completa.

QUESITO 2.3
Conceito 0 – Não abordou o quesito ou o fez de forma totalmente equivocada.
Conceito 1 – Descreveu o modelo de forma apenas superficial, sem desenvolvimento.
Conceito 2 – Desenvolveu uma descrição do modelo de forma parcialmente correta ou insuficiente.
Conceito 3 – Desenvolveu uma descrição do modelo de forma correta e completa.