

EXAMS 4 SUCCESS

SISA

CSPA

Questions & Answers

Certified Security Professional in Artificial Intelligence

(Demo Version - Limited Content)



Version: 6.0

Question: 1

What is a potential risk associated with hallucinations in LLMs, and how should it be addressed to ensure Responsible AI?

- A. Hallucinations can lead to creative outputs, which are beneficial for all applications; hence, no measures are necessary.
- B. Hallucinations cause models to slow down; optimizing hardware performance is necessary to mitigate this issue.
- C. Hallucinations can produce inaccurate or misleading information; it should be addressed by incorporating external knowledge bases and retrieval systems.
- D. Hallucinations are primarily due to overfitting; regularization techniques should be applied during training.

Answer: C

Explanation:

Question: 2

When dealing with the risk of data leakage in LLMs, which of the following actions is most effective in mitigating this issue?

- A. Applying rigorous access controls and anonymization techniques to training data.
- B. Using larger datasets to overshadow sensitive information.
- C. Allowing unrestricted access to training data.
- D. Relying solely on model obfuscation techniques

Answer: A

Explanation:

Question: 3

When deploying LLMs in production, what is a common strategy for parameter-efficient fine-tuning?

- A. Using external reinforcement learning to adjust the model's parameters dynamically.

- B. Freezing the majority of model parameters and only updating a small subset relevant to the task
- C. Training the model from scratch on the target task to achieve optimal performance.
- D. Implementing multiple independent models for each specific task instead of fine tuning a single model

Answer: B

Explanation:

Question: 4

What does the OCTAVE model emphasize in GenAI risk assessment?

- A. Operational Critical Threat, Asset, and Vulnerability Evaluation focused on organizational risks.
- B. Solely technical vulnerabilities in AI models.
- C. Short-term tactical responses over strategic planning.
- D. Exclusion of stakeholder input in assessments.

Answer: A

Explanation:

Question: 5

Which of the following is a potential use case of Generative AI specifically tailored for CXOs (Chief Experience Officers)?

- A. Developing autonomous vehicles for urban mobility solutions.
- B. Automating financial transactions in blockchain networks.
- C. Conducting genetic sequencing for personalized medicine
- D. Enhancing customer support through AI-powered chatbots that provide 24/7 assistance.

Answer: D

Explanation:

EXAMS SUCCESS

Thank you for trying

**Our CSPAI Exam Dumps PDF
Demo**

Try CSPAI practice question

If you want to try CSPAI Exam Practice Test
Questions So go to below link and try it!

<https://www.exams4success.com/cspai/practice-questions>