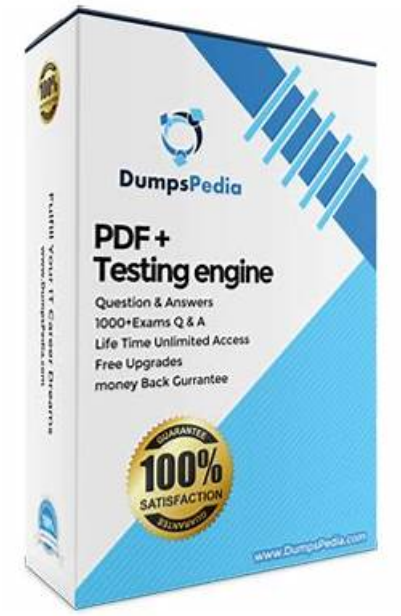
Get Free Updates For SISA CSPAI Exam Dumps Questions



What's more, part of that Prep4SureReview CSPAI dumps now are free: https://drive.google.com/open?id=1TCUOmvmSFTvhcsQG5kN3CIJDFS54ENF3

You must be curious about your exercises after submitting to the system of our CSPAI study materials. Now, we have designed an automatic analysis programs to facilitate your study. You will soon get your learning report without delay. Not only can you review what you have done yesterday on the online engine of the CSPAI study materials, but also can find your wrong answers and mark them clearly. So your error can be corrected quickly. Then you are able to learn new knowledge of the CSPAI Study Materials. Day by day, your ability will be elevated greatly. Intelligent learning helper can relieve your heavy burden. Our CSPAI study materials deserve your purchasing. If you are always waiting and do not action, you will never grow up.

SISA CSPAI Exam Syllabus Topics:

Topic	Details

Topic 1	• Using Gen AI for Improving the Security Posture: This section of the exam measures skills of the Cybersecurity Risk Manager and focuses on how Gen AI tools can strengthen an organization's overall security posture. It includes insights on how automation, predictive analysis, and intelligent threat detection can be used to enhance cyber resilience and operational defense.
Topic 2	• Models for Assessing Gen AI Risk: This section of the exam measures skills of the Cybersecurity Risk Manager and deals with frameworks and models used to evaluate risks associated with deploying generative AI. It includes methods for identifying, quantifying, and mitigating risks from both technical and governance perspectives.
Topic 3	• Securing AI Models and Data: This section of the exam measures skills of the Cybersecurity Risk Manager and focuses on the protection of AI models and the data they consume or generate. Topics include adversarial attacks, data poisoning, model theft, and encryption techniques that help secure the AI lifecycle.

Free PDF 2026 SISA - Real CSPAI Exam

Prep4SureReview's experienced expert team has developed effective training program a for SISA certification CSPAI exam, which is very fit for candidates. Prep4SureReview provide you the high quality product, which can let you do simulation test before the real SISA Certification CSPAI Exam. So you can take a best preparation for the exam.

SISA Certified Security Professional in Artificial Intelligence Sample Questions (Q17-Q22):

NEW QUESTION # 17
Which of the following describes the scenario where an LLM is embedded 'As-is' into an application frame?

- A. Customizing the LLM to fit specific application requirements and workflows before integration.
- B. Replacing the LLM with a more specialized model tailored to the application's needs.
- C. Using the LLM solely for backend data processing, while the application handles all user interactions.
- D. Integrating the LLM into the application without modifications, using its out-of-the-box capabilities directly within the application.

Answer: D

Explanation:
Embedding an LLM 'as-is' means direct integration of the pretrained model into the app framework without alterations, relying on its inherent capabilities for tasks like text generation, simplifying SDLC by avoiding customization overhead. This is suitable for general-purpose apps but may lack optimization for specifics, contrasting with tailored approaches. It accelerates deployment while posing risks like unmitigated biases, necessitating post-integration safeguards. Exact extract: "It describes integrating the LLM without modifications, using out-of-the-box capabilities directly in the application." (Reference: Cyber Security for AI by SISA Study Guide, Section on LLM Integration Methods, Page 110-113).

NEW QUESTION # 18
In line with the US Executive Order on AI, a company's AI application has encountered a security vulnerability. What should be prioritized to align with the order's expectations?

- A. Implementing a rapid response to address and remediate the vulnerability, followed by a review of security practices.
- B. Ignoring the vulnerability if it does not affect core functionalities.
- C. Halting all AI projects until a full investigation is complete.
- D. Immediate public disclosure of the vulnerability.

Answer: A

Explanation:

The US Executive Order on AI emphasizes proactive risk management and robust security to ensure safe AI deployment. When a vulnerability is detected, rapid response to remediate it, coupled with a thorough review of security practices, aligns with these mandates by minimizing harm and preventing recurrence. This approach involves patching the issue, assessing root causes, and updating protocols to strengthen defenses, ensuring compliance with standards like ISO 42001, which prioritizes risk mitigation in AI systems. Public disclosure, while important, is secondary to remediation to avoid premature exposure, and halting projects is overly disruptive unless risks are critical. Ignoring vulnerabilities contradicts responsible AI principles, risking regulatory penalties and trust erosion. This strategy fosters accountability and aligns with governance frameworks for secure AI operations. Exact extract: "Addressing vulnerabilities promptly through remediation and reviewing security practices is prioritized to meet the US Executive Order's expectations for safe and secure AI systems." (Reference: Cyber Security for AI by SISA Study Guide, Section on AI Governance and US EO Compliance, Page 165-168).

NEW QUESTION # 19
What aspect of privacy does ISO 27563 emphasize in AI data processing?

- A. Sharing data freely among AI systems.
- B. Storing all data indefinitely for auditing.
- C. Maximizing data collection for better AI performance.
- D. Consent management and data minimization principles.

Answer: D

Explanation:
ISO 27563 stresses consent management, ensuring informed user agreement, and data minimization, collecting only necessary data to reduce privacy risks in AI processing. These principles prevent overreach and support ethical data handling. Exact extract: "ISO 27563 emphasizes consent management and data minimization in AI data processing for privacy." (Reference: Cyber Security for AI by SISA Study Guide, Section on Privacy Principles in ISO 27563, Page 275-278).

NEW QUESTION # 20
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. Exclusion of stakeholder input in assessments.
- D. Short-term tactical responses over strategic planning.

Answer: A

Explanation:
OCTAVE adapts to GenAI by emphasizing organizational risk perspectives, identifying critical assets like models and data, evaluating threats, and prioritizing mitigations through stakeholder collaboration. It fosters a strategic, enterprise-wide approach to AI risks, integrating business impacts. Exact extract: "OCTAVE emphasizes operational critical threat, asset, and vulnerability evaluation in GenAI risk assessment." (Reference: Cyber Security for AI by SISA Study Guide, Section on OCTAVE for AI, Page 255-258).

NEW QUESTION # 21
In a financial technology company aiming to implement a specialized AI solution, which approach would most effectively leverage existing AI models to address specific industry needs while maintaining efficiency and accuracy?

- A. Using a general Large Language Model (LLM) without adaptation, relying solely on its broad capabilities to handle financial tasks.
- B. Building a new, from scratch Domain-Specific GenAI model for financial tasks without leveraging preexisting models.
- C. Integrating multiple separate Domain-Specific GenAI models for various financial functions without using a foundational model for consistency
- D. Adopting a Foundation Model as the base and fine-tuning it with domain-specific financial data to enhance its capabilities for forecasting and risk assessment.

Answer: D

Explanation:
Leveraging foundation models like GPT or BERT for fintech involves fine-tuning with sector-specific data, such as transaction logs or market trends, to tailor for tasks like risk prediction, ensuring high accuracy without the overhead of scratch-building. This approach maintains efficiency by reusing pretrained weights, reducing training time and resources in SDLC, while domain adaptation mitigates generalization issues. It outperforms unadapted general models or fragmented specifics by providing cohesive, scalable solutions.
Security is enhanced through controlled fine-tuning datasets. Exact extract: "Adopting a Foundation Model and fine-tuning with domain-specific data is most effective for leveraging existing models in fintech, balancing efficiency and accuracy." (Reference: Cyber Security for AI by SISA Study Guide, Section on Model Adaptation in SDLC, Page 105-108).

NEW QUESTION # 22
.....

CSPAI Guide Quiz helped over 98 percent of exam candidates get the certificate. Before you really attend the SISA CSPAI exam and choose your materials, we want to remind you of the importance of holding a certificate like this one. Obtaining a SISA CSPAI certificate likes this one can help you master a lot of agreeable outcomes in the future, like higher salary, the opportunities to promotion and being trusted by the superiors and colleagues.