시험패스가능한CSPAI시험패스인증덤프최신버전덤프샘플문제다운로드

2026 Pass4Test 최신 CSPAI PDF 버전 시험 문제집과 CSPAI 시험 문제 및 답변 무료 공유: https://drive.google.com/open?id=1cxdjg4BCDWH4MfbCCsfFG_7QFu2LWPCX

Pass4Test는 응시자에게 있어서 시간이 정말 소중하다는 것을 잘 알고 있으므로 SISA CSPAI덤프를 자주 업데이트하고, 오래 되고 더 이상 사용 하지 않는 문제들은 바로 삭제해버리며 새로운 최신 문제들을 추가 합니다. 이는 응시자가 확실하고도 빠르게SISA CSPAI덤프를 마스터하고SISA CSPAI시험을 패스할수 있도록 하는 또 하나의 보장입니다.

SISA CSPAI 시험요강:

주제	소개
주제 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.

주제 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.
주제 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.
주제 4	• AIMS and Privacy Standards: ISO 42001 and ISO 27563: This section of the exam measures skills of the AI Security Analyst and addresses international standards related to AI management systems and privacy. It reviews compliance expectations, data governance frameworks, and how these standards help align AI implementation with global privacy and security regulations.

CSPAI최신 업데이트 덤프, CSPAI최고품질 덤프샘플문제 다운

최신 Cyber Security for AI CSPAI 무료샘플문제 (Q41-Q46):

질문 # 41
In transformer models, how does the attention mechanism improve model performance compared to RNNs?

- A. By enabling the model to attend to both nearby and distant words simultaneously, improving its understanding of long-term dependencies
- B. By dynamically assigning importance to every word in the sequence, enabling the model to focus on relevant parts of the input.
- C. By enhancing the model's ability to process data in parallel, ensuring faster training without compromising context.
- D. By processing each input independently, ensuring the model captures all aspects of the sequence equally.

정답：A

설명:
Transformer models leverage self-attention to process entire sequences concurrently, unlike RNNs, which handle inputs sequentially and struggle with long-range dependencies due to vanishing gradients. By computing attention scores across all words, Transformers capture both local and global contexts, enabling better modeling of relationships in tasks like translation or summarization. For example, in a long sentence, attention links distant pronouns to their subjects, improving coherence. This contrasts with RNNs' sequential limitations, which hinder capturing far-apart dependencies. While parallelism (option C) aids efficiency, the core improvement lies in dependency modeling, not just speed. Exact extract: "The attention mechanism enables Transformers to attend to nearby and distant words simultaneously, significantly improving long-term dependency understanding over RNNs." (Reference: Cyber Security for AI by SISA Study Guide, Section on Transformer vs. RNN Architectures, Page 50-53).

질문 # 42
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. 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.
- 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. Using a general Large Language Model (LLM) without adaptation, relying solely on its broad capabilities to handle financial tasks.

정답：A

설명：
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).

질문 # 43
For effective AI risk management, which measure is crucial when dealing with penetration testing and supply chain security?

- A. Prioritize external audits over internal penetration testing to assess supply chain security.
- B. Conduct comprehensive penetration testing and continuously evaluate both internal systems and third- party components in the supply chain.
- C. Perform occasional penetration testing and only address vulnerabilities in the internal network.
- D. Implement penetration testing only for high-risk components and ignore less critical ones

정답：B

설명：
Effective AI risk management requires comprehensive penetration testing and continuous evaluation of both internal and third-party supply chain components to identify vulnerabilities like backdoors or weak APIs. This holistic approach, aligned with SISA risk models, ensures robust security across the AI ecosystem, unlike limited or external-only testing. Exact extract: "Comprehensive penetration testing and continuous evaluation of internal and third-party components are crucial for AI risk management." (Reference: Cyber Security for AI by SISA Study Guide, Section on AI Risk Assessment Models, Page 180-183).

질문 # 44
In utilizing Giskard for vulnerability detection, what is a primary benefit of integrating this open-source tool into the security function?

- A. Limiting its use to only high-priority vulnerabilities.
- B. Enabling real-time detection of vulnerabilities with actionable insights.
- C. Reducing the need for manual vulnerability assessment entirely
- D. Automatically patching vulnerabilities without additional configuration

정답：B

설명：
Giskard, an open-source tool, enhances AI security by enabling real-time vulnerability detection, scanning models for issues like bias or adversarial weaknesses, and providing actionable insights for remediation. This proactive approach supports continuous monitoring, unlike automated patching or limited scopes, and integrates into SDLC for robust security. Exact extract: "Giskard enables real-time detection of vulnerabilities with actionable insights, strengthening AI security functions." (Reference: Cyber Security for AI by SISA Study Guide, Section on Vulnerability Detection Tools, Page 190-193).

질문 # 45
A company's chatbot, Tay, was poisoned by malicious interactions. What is the primary lesson learned from this case study?

- A. Open interaction with users without safeguards can lead to model poisoning and generation of inappropriate content.
- B. Encrypting user data can prevent such attacks
- C. Continuous live training is essential for enhancing chatbot performance.
- D. Chatbots should have limited conversational abilities to prevent poisoning.

정답：A

설명：
The Tay incident, where Microsoft's chatbot was manipulated via toxic inputs to produce offensive content, underscores the dangers of unfiltered live learning, leading to rapid poisoning. Key lesson: Implement safeguards like content filters, rate limits, and moderated feedback loops to prevent adversarial exploitation.
This informs AI security by emphasizing input validation and ethical alignment in interactive systems. Exact extract: "Open interactions without safeguards can lead to model poisoning and inappropriate content, as seen in the Tay case." (Reference: Cyber Security for AI by SISA Study Guide, Section on Case Studies in AI Poisoning, Page 160-163).

질문 # 46
.....