

Reliable CSPAI Exam Topics & Latest CSPAI Exam Questions Vce



SAP C_CPI_2506 SAP Certified Associate - Integration Developer

**Questions & Answers PDF
(Demo Version – Limited Content)**

For More Information – Visit link below:

<https://p2pexam.com/>

Visit us at: <https://p2pexam.com/c-cpi-2506>

2026 Latest Prep4cram CSPAI PDF Dumps and CSPAI Exam Engine Free Share: <https://drive.google.com/open?id=1IHLLhUBHxadViDgeYPLiEHLi-twWCQc>

Why we can produce the best CSPAI exam prep and can get so much praise in the international market. On the one hand, the software version can simulate the real CSPAI examination for you and you can download our study materials on more than one computer with the software version of our study materials. On the other hand, you can finish practicing all the contents in our CSPAI practice materials within 20 to 30 hours. So what are you waiting for? Just rush to buy our CSPAI exam questions!

SISA CSPAI Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">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.
Topic 2	<ul style="list-style-type: none">Improving SDLC Efficiency Using Gen AI: This section of the exam measures skills of the AI Security Analyst and explores how generative AI can be used to streamline the software development life cycle. It emphasizes using AI for code generation, vulnerability identification, and faster remediation, all while ensuring secure development practices.

Topic 3	<ul style="list-style-type: none"> 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 4	<ul style="list-style-type: none"> 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.

>> Reliable CSPAI Exam Topics <<

Reliable CSPAI Exam Topics: 2026 Realistic SISA Latest Certified Security Professional in Artificial Intelligence Exam Questions Vce Pass Guaranteed

Having a SISA Certification CSPAI Exam certificate can help people who are looking for a job get better employment opportunities in the IT field and will also pave the way for a successful IT career for them.

SISA Certified Security Professional in Artificial Intelligence Sample Questions (Q37-Q42):

NEW QUESTION # 37

What is a key benefit of using GenAI for security analytics?

- A. Increasing data silos to protect information.
- B. Limiting analysis to historical data only.
- C. Reducing the use of analytics tools to save costs.
- **D. Predicting future threats through pattern recognition in large datasets.**

Answer: D

Explanation:

GenAI revolutionizes security analytics by mining massive datasets for patterns, predicting emerging threats like zero-day attacks through generative modeling. It synthesizes insights from disparate sources, enabling proactive defenses and anomaly detection with high precision. This foresight allows organizations to allocate resources effectively, preventing breaches before they occur. In practice, it integrates with SIEM systems for enhanced threat hunting. The benefit lies in transforming reactive security into predictive, bolstering posture against sophisticated adversaries. Exact extract: "A key benefit of GenAI in security analytics is predicting future threats via pattern recognition, improving proactive security measures." (Reference: Cyber Security for AI by SISA Study Guide, Section on Predictive Analytics with GenAI, Page 220-223).

NEW QUESTION # 38

Which of the following is a primary goal of enforcing Responsible AI standards and regulations in the development and deployment of LLMs?

- A. Developing AI systems with the highest accuracy regardless of data privacy concerns
- B. Focusing solely on improving the speed and scalability of AI systems
- C. Maximizing model performance while minimizing computational costs.
- **D. Ensuring that AI systems operate safely, ethically, and without causing harm.**

Answer: D

Explanation:

Responsible AI standards, including ISO 42001 for AI management systems, aim to promote ethical development, ensuring safety, fairness, and harm prevention in LLM deployments. This encompasses bias mitigation, transparency, and accountability, aligning with societal values. Regulations like the EU AI Act reinforce this by categorizing risks and mandating safeguards. The goal transcends performance to foster trust and sustainability, addressing issues like discrimination or misuse. Exact extract: "The primary goal is to

ensure AI systems operate safely, ethically, and without causing harm, as outlined in standards like ISO 42001." (Reference: Cyber Security for AI by SISA Study Guide, Section on Responsible AI and ISO Standards, Page 150-153).

NEW QUESTION # 39

In a Retrieval-Augmented Generation (RAG) system, which key step is crucial for ensuring that the generated response is contextually accurate and relevant to the user's question?

- **A. Retrieving relevant information from the vector database before generating a response**
- B. Leveraging a diverse set of data sources to enrich the response with varied perspectives
- C. Utilizing feedback mechanisms to continuously improve the relevance of responses based on user interactions.
- D. Integrating advanced search algorithms to ensure the retrieval of highly relevant documents for context.

Answer: A

Explanation:

In RAG systems, retrieving relevant information from a vector database before generation is pivotal, as it grounds responses in verified, contextually aligned data. Using embeddings and similarity metrics, the system fetches documents matching the query's intent, ensuring accuracy and relevance. While diverse sources or feedback aid long-term improvement, the retrieval step directly drives contextual fidelity, streamlining SDLC by modularizing data access. Exact extract: "Retrieving relevant information from the vector database is crucial for ensuring contextually accurate responses in RAG systems." (Reference: Cyber Security for AI by SISA Study Guide, Section on RAG Optimization, Page 120-123).

NEW QUESTION # 40

A company developing AI-driven medical diagnostic tools is expanding into the European market. To ensure compliance with local regulations, what should be the company's primary focus in adhering to the EU AI Act?

- **A. Implementing measures to prevent any harmful outcomes and ensure AI system safety**
- B. Prioritizing transparency and accountability in AI systems to avoid high-risk categorization
- C. Focusing on integrating ethical guidelines to ensure AI decisions are fair and unbiased.
- D. Ensuring the AI system meets stringent privacy standards to protect sensitive data

Answer: A

Explanation:

The EU AI Act classifies AI systems by risk, with medical diagnostics as high-risk, requiring stringent safety measures to prevent harm, such as misdiagnoses. Compliance prioritizes robust testing, validation, and monitoring to ensure safe outcomes, aligning with ISO 42001's risk management framework. While ethics and privacy are critical, safety is the primary focus to meet regulatory thresholds and protect users. Exact extract: "The EU AI Act emphasizes implementing measures to prevent harmful outcomes and ensure AI system safety, particularly for high-risk applications like medical diagnostics." (Reference: Cyber Security for AI by SISA Study Guide, Section on EU AI Act Compliance, Page 175-178).

NEW QUESTION # 41

In ISO 42001, what is required for AI risk treatment?

- A. Focusing only on post-deployment risks.
- **B. Identifying, analyzing, and evaluating AI-specific risks with treatment plans.**
- C. Ignoring risks below a certain threshold.
- D. Delegating all risk management to external auditors.

Answer: B

Explanation:

ISO 42001 mandates a systematic risk treatment process, involving identification of AI risks (e.g., bias, security), analysis of impacts, evaluation against criteria, and development of treatment plans like mitigation or acceptance. This ensures proactive management throughout the AI lifecycle. Exact extract: "ISO 42001 requires identifying, analyzing, and evaluating AI risks with appropriate treatment plans." (Reference: Cyber Security for AI by SISA Study Guide, Section on Risk Treatment in ISO 42001, Page 270-273).

• • • • •

Latest CSPAI Exam Questions Vce: https://www.prep4cram.com/CSPAI_exam-questions.html

- What's more, part of that Prep4cram CSPAI dumps now are free: <https://drive.google.com/open?id=1IHLLhUBHxadViDgeYPlEHLIi-twWCQc>

id=1IHLLhUBHxadViDgeYPLiEHLi-twWCQc