

Exam CSPAI Certification Cost, Original CSPAI Questions



P.S. Free 2026 SISA CSPAI dumps are available on Google Drive shared by Prep4away: <https://drive.google.com/open?id=1fZKGsWcDLPJOnmqK9RWwC29ehZJ5EZwh>

We cannot predicate the future but we can live in the moment. There are many meaningful things waiting for us to do. Try to immerse yourself in new experience. Once you get the CSPAI certificate, your life will change greatly. First of all, you will grow into a comprehensive talent under the guidance of our CSPAI Exam Materials, which is very popular in the job market. And you will get better jobs for your CSPAI certification as well.

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">Evolution of Gen AI and Its Impact: This section of the exam measures skills of the AI Security Analyst and covers how generative AI has evolved over time and the implications of this evolution for cybersecurity. It focuses on understanding the broader impact of Gen AI technologies on security operations, threat landscapes, and risk management strategies.
Topic 5	<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.

Original CSPAI Questions - CSPAI Latest Test Format

People always want to prove that they are competent and skillful in some certain area. The ways to prove their competences are varied but the most direct and convenient method is to attend the CSPAI certification exam and get some certificate. Passing the CSPAI certification can prove that you are very competent and excellent and you can also master useful knowledge and skill through passing the CSPAI test. Purchasing our CSPAI guide torrent can help you pass the CSPAI exam and it costs little time and energy.

SISA Certified Security Professional in Artificial Intelligence Sample Questions (Q41-Q46):

NEW QUESTION # 41

What role does GenAI play in automating vulnerability scanning and remediation processes?

- A. By generating code patches and suggesting fixes based on vulnerability descriptions.
- B. By compiling lists of vulnerabilities without any analysis.
- C. By increasing the frequency of manual scans to ensure thoroughness.
- D. By ignoring low-priority vulnerabilities to focus on high-impact ones.

Answer: A

Explanation:

GenAI automates vulnerability management by analyzing scan results and generating tailored code patches or remediation strategies, accelerating the fix process and reducing human error. Using natural language processing, it interprets vulnerability reports, cross-references with known exploits, and proposes secure code alternatives, integrating seamlessly into DevSecOps pipelines. This proactive approach minimizes exposure windows and enhances system resilience against exploits. For instance, in cloud environments, GenAI can simulate patch impacts before application. This contributes to a stronger security posture by enabling rapid, accurate responses to threats. Exact extract: "GenAI automates vulnerability scanning and remediation by generating code patches and fixes, improving efficiency and security posture." (Reference: Cyber Security for AI by SISA Study Guide, Section on Automation in Vulnerability Management, Page 205-208).

NEW QUESTION # 42

How does the STRIDE model adapt to assessing threats in GenAI?

- A. By applying Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege to AI components.
- B. By focusing only on hardware threats in AI systems.
- C. By excluding AI-specific threats like model inversion.
- D. By using it unchanged from traditional software.

Answer: A

Explanation:

The STRIDE model adapts to GenAI by evaluating threats across its categories: Spoofing (e.g., fake inputs), Tampering (e.g., data poisoning), Repudiation (e.g., untraceable generations), Information Disclosure (e.g., leakage from prompts), Denial of Service (e.g., resource exhaustion), and Elevation of Privilege (e.g., jailbreaking). This systematic threat modeling helps in designing resilient GenAI systems, incorporating AI-unique aspects like adversarial inputs. Exact extract: "STRIDE adapts to GenAI by applying its threat categories to AI components, assessing specific risks like tampering or disclosure." (Reference: Cyber Security for AI by SISA Study Guide, Section on Threat Modeling for GenAI, Page 240-243).

NEW QUESTION # 43

What is the main objective of ISO 42001 in AI management systems?

- A. To establish requirements for an AI management system within organizations.
- B. To focus solely on technical specifications for AI algorithms.
- C. To regulate hardware used in AI deployments.

- D. To provide guidelines only for small-scale AI projects.

Answer: A

Explanation:

ISO 42001 outlines a framework for organizations to manage AI responsibly, covering risk assessment, governance, and continual improvement. It ensures alignment with ethical principles, promoting trustworthy AI through structured processes. Applicable across sectors, it integrates with existing management systems like ISO 27001. Exact extract: "The main objective of ISO 42001 is to establish requirements for an AI management system in organizations." (Reference: Cyber Security for AI by SISA Study Guide, Section on ISO 42001 Overview, Page 260-263).

NEW QUESTION # 44

In assessing GenAI supply chain risks, what is a critical consideration?

- A. Focusing only on internal development risks.
- B. Ignoring open-source dependencies to reduce complexity.
- C. Evaluating third-party components for embedded vulnerabilities.
- D. Assuming all vendors comply with standards automatically.

Answer: C

Explanation:

GenAI supply chain risk assessment prioritizes scrutinizing third-party libraries, datasets, and models for vulnerabilities like backdoors or biases, using tools for dependency scanning. This holistic view prevents cascade failures, as seen in compromised pretrained models. Mitigation includes vendor audits and secure sourcing. Exact extract: "A critical consideration in GenAI supply chain risks is evaluating third-party components for vulnerabilities." (Reference: Cyber Security for AI by SISA Study Guide, Section on Supply Chain Risk Assessment, Page 250-253).

NEW QUESTION # 45

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

Answer: D

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 # 46

.....

Customers of Prep4away will also receive updates for 1 year after purchase. A lot of students have prepared from the for the Certified Security Professional in Artificial Intelligence (CSPAI) certification test and passed it in a single try. They have rated the Certified Security Professional in Artificial Intelligence (CSPAI) as one of the best in the market to prepare for the CSPAI exam in minimum time. Try a free demo now and start your journey towards your dream certification!

Original CSPAI Questions: <https://www.prep4away.com/SISA-certification/braindumps.CSPAI.etc.file.html>

- Interactive CSPAI EBook ☐ CSPAI Dumps Collection ☐ CSPAI New Braindumps Free ☐ Open website {

Free PDF Quiz 2026 CSPAI: Certified Security Professional in Artificial Intelligence Fantastic Exam Certification Cost ☐
Go to website > www.pdfvce.com ☐ open and search for ➡ CSPAI ☐☐ to download for free ☐ CSPAI Valid Exam Preparation

- BTW, DOWNLOAD part of Prep4away CSPA dumps from Cloud Storage: <https://drive.google.com/open?id=1fZKGsWcDLPJOnmqK9RWwC29ehZJ5EZwh>

BTW, DOWNLOAD part of Prep4away CSPA dumps from Cloud Storage: <https://drive.google.com/open?id=1fZKGsWcDLPJOnmqK9RWwC29ehZJ5EZwh>