DBCLOUD
EXAMS

QUESTIONS & ANSWERS

verified



Technology Provider: CompTIA

Exam: CompTIA SecAI+

Number of questions in the database: 169

Exam Version: NOV.2026

Question #1 Topic1

Which of the following job roles in an organizational governance structure develops a model from business use cases?

A. Platform architect

B. AI risk analyst

C. Machine learning operations (MLOps) engineer

D. Data scientist

Correct Answer: D

Question #2 Topic1

An administrator, who works for a financial institution, is required to implement data security controls for data at rest within AI systems that involve data disclosure. Which of the following is the most suitable control?

A. Data lineage

B. Rate limits

C. Encryption

D. Masking

Correct Answer: C

https://dbcloud.academy/

Question #3 Topic1

A security engineer needs to monitor an AI-based system for runtime operations. The engineer is mostly concerned about the visibility of internal activity. Which of the following is the most appropriate monitoring solution?

A. Deploying a security information and event management (SIEM) tool

B. Implementing a web application firewall (WAF) with header logging

C. Relying on vendor model controls and monitoring prompt inputs

D. Enabling stack call and debugging level traces at the function level

Correct Answer: D

Question #4 Topic1

Which of the following should an auditor reference when reviewing a company's human resources AI systems for legal non-compliance?

A. Organization for Economic Cooperation and Development (OECD) standard

B. National Institute of Standards and Technology (NIST) AI Risk Management Framework 9RMF)

C. European Union (EU) AI Act

D. International Organization for Standardization (ISO)

Correct Answer: C

Question #5 Topic1

An airline corporation wants to implement a chatbot application using a large language model (LLM) so its customers:

Can ask question and receive answers about flight details.

Have the option to upload files.

Which of the following security controls should the airline use to protect against malicious input and unauthorized use beyond the service-level agreement? (Choose two.)

A. Prompt guardrails

B. Role-based access controls

C. Firewall rules

D. Model token quotas

Correct Answer: AD

https://dbcloud.academy/