Vendor: CompTIA

Exam Code: CY0-001

Exam Name: CompTIA SecAI+ Certification Exam

Version: DEMO

QUESTION 1
An organization is concerned with the exposure of sensitive data. Which of the following is the **most** relevant security concern?

A. Overfitting
B. Model inversion
C. Data normalization
D. Hyperparameter tuning

Answer: B
Explanation:
Model inversion is a security concern where attackers can reconstruct or infer sensitive training data from the AI model's outputs. This directly threatens data confidentiality, making it the most relevant concern for sensitive data exposure.

QUESTION 2
Faculty members at a university are concerned about potential inherent bias and inconsistency in one department's AI plagiarism detection service.
Which of the following principles will **most** likely to address their concerns?

A. Transparency
B. Explainability
C. Consistency
D. Accountability

Answer: C
Explanation:
Consistency ensures that an AI system applies rules and produces results in a uniform manner across all cases. This principle directly addresses concerns about bias and irregular outcomes in the plagiarism detection service.

QUESTION 3
A security administrator must provide access controls for AI systems to list tables. Which of the following should the administrator implement?

A. Agentic AI access
B. Network access control list (NACL)
C. Model access
D. Data access

Answer: D
Explanation:
Since the requirement is to control which users or systems can list tables, the proper control lies at the data access level. Implementing data access controls ensures only authorized entities can view or query the underlying tables used by the AI system.

QUESTION 4
A machine learning (ML) engineer is working with a security engineer to identify the best practices for securing a system with various AI models.
Which of the following actions should the engineers suggest?

A. Conducting guardrail testing and security validation
B. Following a secure model development life cycle (MDLC)
C. Implementing comprehensive security architecture
D. Using a secure software development life cycle (SDLC)

Answer: B
Explanation:
A secure MDLC is tailored to AI and ML systems, ensuring security is integrated throughout the model's design, training, validation, deployment, and monitoring phases. This directly addresses best practices for securing systems with AI models.

QUESTION 5
Which of the following is an example of how a security analyst uses generative AI in the triage process?

A. To predict the next attack target with higher accuracy
B. To use statistical analysis for malicious code assessment
C. To summarize security findings by category
D. To tag malware using machine learning (ML) algorithms

Answer: C
Explanation:
In triage, generative AI is most effective for quickly summarizing and categorizing large volumes of alerts or findings. This helps analysts prioritize incidents and streamline the investigation process.

QUESTION 6
A company develops an AI model to diagnose patients. Hospitals access the model through an integrated application programming interface (API). The security team performs a denial-of-service (DoS) attack via brute force on the model. Which of the following controls would have prevented this issue?

A. Tokenization
B. Model guardrails
C. Rate limiting
D. Prompt firewall

Answer: C
Explanation:
Rate limiting restricts the number of API requests within a specific timeframe, preventing brute-force attempts that can overwhelm the AI model and cause denial-of-service conditions.

QUESTION 7
A security team is using an AI-based tool to try to bypass organizational boundaries. The team uses AI to look at the current state and suggest different attack vectors based on the outcome of the previous ones. Which of the following techniques is the team most likely using?

A. Manual signature matching
B. Code quality testing
C. Fraud detection

D. Automated penetration testing

Answer: D
Explanation:
The described behavior - iteratively assessing the environment and adapting attack paths based on prior outcomes - matches automated penetration testing, where AI-driven tools simulate attack chains and adjust tactics dynamically.

QUESTION 8
Which of the following attacks would be the best to automate with AI during dynamic application software testing (DAST)?

A. Distributed denial-of-service (DDoS)
B. Data poisoning
C. Payload creation
D. Threat modeling

Answer: C
Explanation:
During DAST, automating the generation of diverse, targeted attack payloads lets testers probe runtime inputs (e.g., XSS, SQLi, command injection) more thoroughly and discover vulnerabilities that manual or static tests might miss.

QUESTION 9
A disgruntled employee changed the company policies that a chatbot references in order to create confusion and disrupt the business. Which of the following AI-generated vulnerabilities is the employee exploiting?

A. Data reduction
B. Data masking
C. Data poisoning
D. Data leaking

Answer: C
Explanation:
Altering the source data (policy content) that the chatbot relies on corrupts its knowledge and behavior, which is characteristic of data poisoning attacks.

QUESTION 10
A security consultant must summarize the impact of posture management on a machine learning (ML) use case. Which of the following is the most appropriate reference for this purpose?

A. Organization for Economic Co-operation and Development (OECD) standards
B. National Institute of Standards and Technology (NIST) AI Risk Management Framework (RMF)
C. European Union AI Act
D. Generative adversarial network (GAN)

Answer: B
Explanation:
The NIST AI RMF provides structured guidance for assessing and managing risks across the AI lifecycle, including posture management. It helps organizations align AI security practices with

governance, resilience, and trustworthiness requirements.

QUESTION 11
A cybersecurity analyst must use pattern recognition on a data set containing unstructured data. Which of the following models is the **best** for this task?

A. Long short-term memory
B. Convolutional neural network
C. Decision tree
D. Logistic regression

Answer: B
Explanation:
Convolutional neural networks (CNNs) are highly effective at detecting patterns in unstructured data such as images, audio, or text embeddings. Their ability to automatically learn spatial or hierarchical features makes them the best choice for pattern recognition on unstructured datasets.

QUESTION 12
An employee wants a consulting company to procure a data set that contains age, ethnicity, and diabetes status. During development, the employer wants to ensure the integrity of the data. Which of the following is the **best** strategy to accomplish this task?

A. Implementing checksums
B. Conducting human evaluation
C. Querying the model
D. Enabling log monitoring

Answer: A
Explanation:
Checksums ensure data integrity by detecting any unauthorized or accidental changes to the dataset. This provides a reliable way to confirm that sensitive attributes such as age, ethnicity, and diabetes status remain unaltered during development.

QUESTION 13
Which of the following strengthens the performance of a large language model (LLM) for malicious reconnaissance?

A. Enhancing a foundational model with the inclusion of retrieval-augmented generation (RAG)
B. Creating a web scraper script using AI to capture the company website
C. Instructing an AI assistant to query as an administrator
D. Prompting a chatbot to describe server naming patterns and Internet Protocol (IP) ranges

Answer: A
Explanation:
RAG augments an LLM with external, up-to-date information retrieval, improving its factual accuracy and contextual scope—capabilities that directly strengthen the model's effectiveness for reconnaissance.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**