

# CY0-001 Buch - CY0-001 Prüfungsfragen



Sie haben schon die Prüfungsmaterialien zur CompTIA CY0-001 Zertifizierung von ExamFragen gesehen. Es ist doch Zeit, eine Wahl zu treffen. Sie können auch andere Produkte wählen, aber unser ExamFragen wird Ihnen die größten Interessen bringen. Mit ExamFragen werden Sie eine glänzende Zukunft haben, eine bessere Berufsaussichten in der IT-Branche haben und effizient arbeiten.

Die CompTIA CY0-001 Zertifizierungsprüfungen werden normalerweise von den IT-Spezialisten gemäß ihren Berufserfahrungen bearbeitet. So ist es auch bei ExamFragen. Die IT-Experten bieten Ihnen CompTIA CY0-001 Prüfungsfragen und Antworten (CompTIA SecAI+ Certification Exam), mit deren Hilfe Sie die Prüfung erfolgreich bestehen können. Die Genauigkeit von unseren Prüfungsfragen und Antworten beträgt 100%. Mit ExamFragen Produkten können Sie ganz leicht die CompTIA CY0-001 Zertifikate bekommen, was Ihnen eine große Beförderung in der IT-Branche ist.

>> CY0-001 Buch <<

## CY0-001 Prüfungsfragen, CY0-001 PDF Demo

Wenn Sie sich noch anstrengend um die CY0-001 Zertifizierungsprüfung bemühen, dann kann ExamFragen in diesem Moment Ihnen helfen, Problem zu lösen. ExamFragen bietet Ihnen Schulungsunterlagen von hoher Qualität, damit Sie die Prüfung bestehen und exzellentes Mitglied der CompTIA CY0-001 Zertifizierung werden können. Wenn Sie sich entscheiden, durch die CompTIA CY0-001 Zertifizierungsprüfung sich zu verbessern, dann wählen Sie bitte ExamFragen. ExamFragen zu wählen ist keinesfalls nicht falsch. Unser ExamFragen verspricht, dass Sie beim ersten Versuch die CompTIA CY0-001 Zertifizierungsprüfung bestehen und somit das Zertifikat bekommen können. So können Sie sich sicher verbessern.

## CompTIA SecAI+ Certification Exam CY0-001 Prüfungsfragen mit Lösungen (Q80-Q85):

### 80. Frage

A line of business wants to onboard an application that uses a custom AI model for employee assessments. The Chief Information Officer (CIO) agrees to allow the engagement to proceed but first wants a threat model. Which of the following is the most appropriate to use for an AI threat model?

- A. Organization for Economic Co-operation and Development (OECD)
- **B. Adversarial Threat Landscape for AI Systems (ATLAS)**
- C. Responsible AI
- D. International Organization for Standardization (ISO)

**Antwort: B**

**Begründung:**

ATLAS is specifically designed for creating AI threat models. It catalogs adversarial techniques, tactics, and use cases that target AI systems, making it the most appropriate framework for assessing risks to a custom AI model in employee assessments.

### 81. Frage

During the selection of a machine learning (ML)-based threat classification model, a cybersecurity administrator verifies that label distribution is highly unbalanced. Which of the following processing techniques should the engineer use to balance the model?

- A. Data provenance
- B. Data verification
- C. Data lineage
- **D. Data augmentation**

**Antwort: D**

Begründung:

When label distribution is highly unbalanced, data augmentation generates additional synthetic samples for the underrepresented classes. This balances the dataset, improving the ML model's ability to classify threats accurately across all categories.

### 82. Frage

A cybersecurity analyst wants to choose a machine learning (ML) model to classify log entries while providing the best explainability. Which of the following models should the analyst use?

- **A. Decision trees**
- B. Generative adversarial network (GAN)
- C. Large language model (LLM)
- D. Neural networks

**Antwort: A**

Begründung:

Decision trees provide clear and interpretable decision paths, making them highly explainable compared to complex models like neural networks or GANs. This makes them the best choice for classifying log entries when explainability is a priority.

### 83. Frage

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

- **A. Data scientist**
- B. Platform architect
- C. Machine learning operations (MLOps) engineer
- D. AI risk analyst

**Antwort: A**

Begründung:

A data scientist develops models from business use cases by translating organizational needs into machine learning solutions. They prepare data, select algorithms, and build models that align with the use cases.

### 84. Frage

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. Rate limiting**
- B. Tokenization
- C. Prompt firewall
- D. Model guardrails

**Antwort: A**

Begründung:

- [illegible]

