

CS0-002^{Q&As}

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-002 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/cs0-002.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1

A security architect is reviewing the options for performing input validation on incoming web form submissions. Which of the following should the architect as the MOST secure and manageable option?

- A. Client-side whitelisting
- B. Server-side whitelisting
- C. Server-side blacklisting
- D. Client-side blacklisting

Correct Answer: B

QUESTION 2

A Chief Executive Officer (CEO) is concerned about the company's intellectual property being leaked to competitors. The security team performed an extensive review but did not find any indication of an outside breach. The data sets are currently encrypted using the Triple Data Encryption Algorithm. Which of the following courses of action is appropriate?

- A. Limit all access to the sensitive data based on geographic access requirements with strict role-based access controls.
- B. Enable data masking and reencrypt the data sets using AES-256.
- C. Ensure the data is correctly classified and labeled, and that DLP rules are appropriate to prevent disclosure.
- D. Use data tokenization on sensitive fields, reencrypt the data sets using AES-256, and then create an MD5 hash.

Correct Answer: C

QUESTION 3

An organization that uses SPF has been notified emails sent via its authorized third-party partner are getting rejected. A security analyst reviews the DNS entry and sees the following: `v=spf1 ip4:180.10.6.5 ip4:180.10.6.10 include:robustmail.com ~all` The organization's primary mail server IP is 180.10.6.6, and the secondary mail server IP is 180.10.6.5. The organization's third-party mail provider is "Robust Mail" with the domain name robustmail.com. Which of the following is the MOST

likely reason for the rejected emails?

- A. SPF version 1 does not support third-party providers.
- B. The primary and secondary email server IP addresses are out of sequence.
- C. An incorrect IP version is being used.
- D. The wrong domain name is in the SPF record.

Correct Answer: D

QUESTION 4

During the threat modeling process for a new application that a company is launching, a security analyst needs to define methods and items to take into consideration. Which of the following are part of a known threat modeling method?

- A. Threat profile, infrastructure and application vulnerabilities, security strategy and plans
- B. Purpose, objective, scope, (earn management, cost, roles and responsibilities
- C. Spoofing tampering, repudiation, information disclosure, denial of service elevation of privilege
- D. Human impact, adversary's motivation, adversary's resources, adversary's methods

Correct Answer: C

QUESTION 5

Forming a hypothesis, looking for indicators of compromise, and using the findings to proactively improve detection capabilities are examples of the value of:

- A. vulnerability scanning.
- B. threat hunting.
- C. red learning.
- D. penetration testing.

Correct Answer: B

[Latest CS0-002 Dumps](#)

[CS0-002 PDF Dumps](#)

[CS0-002 Study Guide](#)