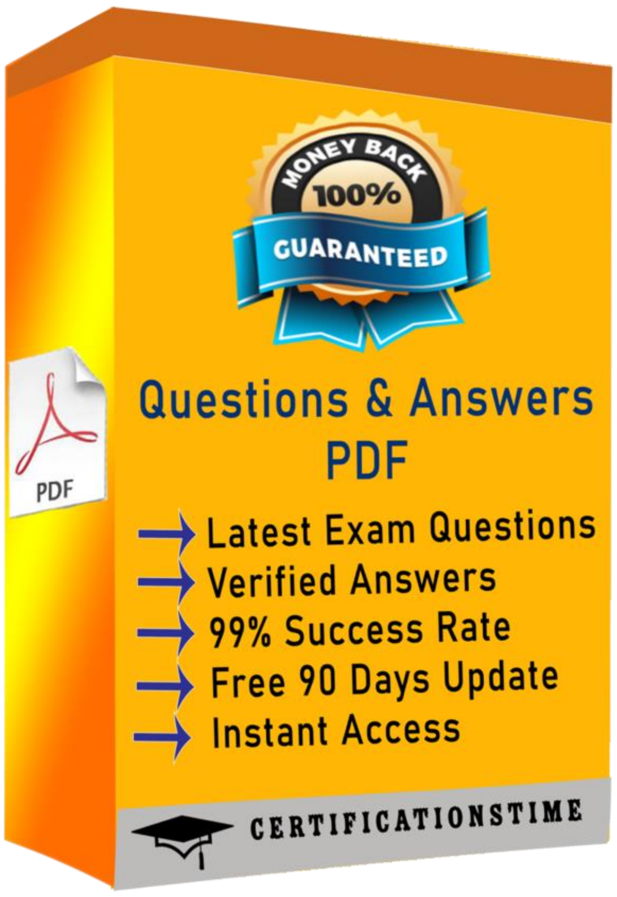
# CompTIA

# Exam Questions CS0-002

## CompTIA Cybersecurity Analyst (CySA+)

https://certificationstime.com/



## QUESTION 1

A company's modem response team is handling a threat that was identified on the network Security

analysts have as at remote sites. Which of the following is the MOST appropriate next step in the

incident response plan?

A. Quarantine the web server

B. Deploy virtual firewalls

C. Capture a forensic image of the memory and disk

D. Enable web server containerization

**Correct Answer: B**

## QUESTION 2

Which of the following should be found within an organization's acceptable use policy?

A. Passwords must be eight characters in length and contain at least one special character.

B. Customer data must be handled properly, stored on company servers, and encrypted when

possible

C. Administrator accounts must be audited monthly, and inactive accounts should be removed

D. Consequences of violating the policy could include discipline up to and including termination.

Correct Answer: D

## QUESTION 3

A company was recently awarded several large government contracts and wants to determine its

current risk from one specific APT.

Which of the following threat modeling methodologies would be the MOST appropriate to use during

this analysis?

A. Attack vectors

B. Adversary capability

C. Diamond Model of Intrusion Analysis

D. Kill chain

E. Total attack surface

Correct Answer: B

**QUESTION 4**

Which of the following roles is ultimately responsible for determining the classification levels assigned

to specific data sets?

A. Data custodian

B. Data owner

C. Data processor

D. Senior management

Correct Answer: B

**QUESTION 5**

A cybersecurity analyst is contributing to a team hunt on an organization's endpoints.

Which of the following should the analyst do FIRST?

A. Write detection logic.

B. Establish a hypothesis.

C. Profile the threat actors and activities

D. Perform a process analysis

https://certificationstime.com/updated/cs0-002-exam-dumps-pdf/

Correct Answer: C

**QUESTION 6**

A security analyst discovers accounts in sensitive SaaS-based systems are not being removed in a

timely manner when an employee leaves the organization To BEST resolve the issue, the organization

should implement

A. federated authentication

B. role-based access control.

C. manual account reviews

D. multifactor authentication.

Correct Answer: A

**QUESTION 7**

A cybersecurity analyst is supporting an incident response effort via threat intelligence. Which of the

following is the analyst MOST likely executing?

A. Requirements analysis and collection planning

B. Containment and eradication

C. Recovery and post-incident review

D. Indicator enrichment and research pivoting

Correct Answer: A

## Full Access:

**https://certificationstime.com/updated/cs0-002-exam-dumps-pdf/**