CS0-003 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

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

https://www.pass4itsure.com/cs0-003.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

The Chief Information Security Officer wants to eliminate and reduce shadow IT in the enterprise. Several high-risk cloud applications are used that increase the risk to the organization. Which of the following solutions will assist in reducing the risk?

A. Deploy a CASB and enable policy enforcement

B. Configure MFA with strict access

C. Deploy an API gateway

D. Enable SSO to the cloud applications

Correct Answer: A

A cloud access security broker (CASB) is a tool that can help reduce the risk of shadow IT in the enterprise by providing visibility and control over cloud applications and services. A CASB can enable policy enforcement by blocking unauthorized or risky cloud applications, enforcing data loss prevention rules, encrypting sensitive data, and detecting anomalous user behavior.

QUESTION 2

The SFTP server logs show thousands of failed login attempts from hundreds of IP addresses worldwide. Which of the following controls would BEST protect the service?

A. Whitelisting authorized IP addresses

B. Blacklisting unauthorized IP addresses

C. Enforcing more complex password requirements

D. Establishing a sinkhole service

Correct Answer: A

QUESTION 3

A company is aiming to test a new incident response plan. The management team has made it clear that the initial test should have no impact on the environment. The company has limited resources to support testing. Which of the following exercises would be the best approach?

A. Tabletop scenarios

B. Capture the flag

C. Red team vs. blue team

D. Unknown-environment penetration test

Correct Answer: A

A tabletop scenario is an informal, discussion-based session in which a team discusses their roles and responses during an emergency, walking through one or more example scenarios. A tabletop scenario is the best approach for a company that wants to test a new incident response plan without impacting the environment or using many resources. A tabletop scenario can help the company identify strengths and weaknesses in their plan, clarify roles and responsibilities, and improve communication and coordination among team members. The other options are more intensive and disruptive exercises that involve simulating a real incident or attack. CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 16; https://www.linkedin.com/pulse/tabletop-exercises-explained-matt-lemon-phd

QUESTION 4

As a proactive threat-hunting technique, hunters must develop situational cases based on likely attack scenarios derived from the available threat intelligence information. After forming the basis of the scenario, which of the following may the threat hunter construct to establish a framework for threat assessment?

A. Critical asset list

B. Threat vector

C. Attack profile

D. Hypothesis

Correct Answer: D

A hypothesis is a statement that can be tested by threat hunters to establish a framework for threat assessment. A hypothesis is based on situational awareness and threat intelligence information, and describes a possible attack scenario that may affect the organization. A hypothesis can help to guide threat hunters in their investigation by providing a clear and specific question to ans" there any evidence of lateral" https://www.crowdstrike.com/blog/tech-center/threat-huntinghypothesisdevelopment/

QUESTION 5

An organization has deployed a cloud-based storage system for shared data that is in phase two of the data life cycle. Which of the following controls should the security team ensure are addressed? (Choose two.)

A. Data classification

B. Data destruction

C. Data loss prevention

D. Encryption

E. Backups

F. Access controls

Correct Answer: CD

This question is about management of data security and compliance in the cloud with regard to data life cycle.

DLP - Azure, GCP, and AWS have many resources and tools available to identify confidential data in use, in storage,

and in transit and then understand how that data is used to protect it in a shared data environment.

Encryption - is used to protect the data at rest on storage devices, in transit, and even in use. It protects connectivity to the cloud, data stored in the could, etc...

Both DLP and Encryption is a part of the data life cycle management.