CS0-003Q&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.pass2lead.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

A technician identifies a vulnerability on a server and applies a software patch. Which of the following should be the next step in the remediation process?

A. Testing

B. Implementation

C. Validation

D. Rollback

Correct Answer: C

The next step in the remediation process after applying a software patch is validation. Validation is a process that involves verifying that the patch has been successfully applied, that it has fixed the vulnerability, and that it has not caused any adverse effects on the system or application functionality or performance. Validation can be done using various methods, such as scanning, testing, monitoring, or auditing.

QUESTION 2

A malicious actor has gained access to an internal network by means of social engineering. The actor does not want to lose access in order to continue the attack. Which of the following best describes the current stage of the Cyber Kill Chain that the threat actor is currently operating in?

A. Weaponization

B. Reconnaissance

C. Delivery

D. Exploitation

Correct Answer: D

The Cyber Kill Chain is a framework that describes the stages of a cyberattack from reconnaissance to actions on objectives. The exploitation stage is where attackers take advantage of the vulnerabilities they have discovered in previous stages to further infiltrate a" objectives. In this case, the malicious actor has gained access to an internal network by means of social engineering and does not want to lose access in order to continue the attack. This indicates that the actor is in the exploitation stage of the Cyber Kill Chain. Official Reference: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

QUESTION 3

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.

QUESTION 4

A security team is struggling with alert fatigue, and the Chief Information Security Officer has decided to purchase a SOAR platform to alleviate this issue. Which of the following BEST describes how a SOAR platform will help the security team?

A. SOAR will integrate threat intelligence into the alerts, which will help the security team decide which events should be investigated first.

B. A SOAR platform connects the SOC with the asset database, enabling the security team to make informed decisions immediately based on asset criticality.

C. The security team will be able to use the SOAR framework to integrate the SIEM with a TAXII server, which has an automated intelligence feed that will enhance the alert data.

D. Logic can now be created that will allow the SOAR platform to block specific traffic at the firewall according to predefined event triggers and actions.

Correct Answer: A

QUESTION 5

Which of the following best describes the reporting metric that should be utilized when measuring the degree to which a system, application, or user base is affected by an uptime availability outage?

A. Timeline

B. Evidence

C. Impact

D. Scope

Correct Answer: C

The impact metric is the best way to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The impact metric quantifies the consequences of the outage in terms of lost revenue, productivity, reputation, customer satisfaction, or other relevant factors. The impact metric can help prioritize the recovery efforts and justify the resources needed to restore the service.The other options are not the best ways to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The timeline metric (A) measures the duration and frequency of the outage, but not its effects. The evidence metric (B) measures the sources and types of data that can be used to investigate and analyze the outage, but not its effects. The scope metric (D) measures the extent and severity of the outage, but not its effects.