CS0-002 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-002 Exam with 100% Guarantee

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

https://www.pass4itsure.com/cs0-002.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which of the following ICS network protocols has no inherent security functions on TCP port 502?

A. CIP

B. DHCP

C. SSH

D. Modbus

Correct Answer: D

QUESTION 2

Due to new regulations, a company has decided to institute an organizational vulnerability management program and assign the function to the security team. Which of the following frameworks would BEST support the program? (Select two.)

A. COBIT

B. NIST

C. ISO 27000 series

D. ITIL

E. OWASP

Correct Answer: BD

QUESTION 3

After a breach involving the exfiltration of a large amount of sensitive data a security analyst is reviewing the following firewall logs to determine how the breach occurred:

```
1286  ?   Ss   0:00   /usr/sbin/cupsd -f
1287  ?   Ss   0:00   /usr/sbin/httpd
1297  ?   Ssl  0:00   /usr/bin/libvirtd
1301  ?   Ss   0:00   ./usr/sbin/sshd -D
1308  ?   Ss   0:00   /usr/sbin/atd -f
```

Which of the following IP addresses does the analyst need to investigate further?

A. 192.168.1.1

B. 192.168.1.10

C. 192.168.1.12

D. 192.168.1.193

Correct Answer: C

QUESTION 4

A security audit revealed that port 389 has been used instead of 636 when connecting to LDAP for the authentication of users. The remediation recommended by the audit was to switch the port to 636 wherever technically possible. Which of the following is the BEST response?

A. Correct the audit. This finding is a well-known false positive; the services that typically run on 389 and 636 are identical.

B. Change all devices and servers that support it to 636, as encrypted services run by default on 636.

C. Change all devices and servers that support it to 636, as 389 is a reserved port that requires root access and can expose the server to privilege escalation attacks.

D. Correct the audit. This finding is accurate, but the correct remediation is to update encryption keys on each of the servers to match port 636.

Correct Answer: B

QUESTION 5

A company\\'s Chief Information Officer wants to use a CASB solution to ensure policies are being met during cloud access. Due to the nature of the company\\'s business and risk appetite, the management team elected to not store financial information in the cloud. A security analyst needs to recommend a solution to mitigate the threat of financial data leakage into the cloud. Which of the following should the analyst recommend?

A. Utilize the CASB to enforce DLP data-at-rest protection for financial information that is stored on premises.

B. Do not utilize the CASB solution for this purpose, but add DLP on premises for data in motion.

C. Utilize the CASB to enforce DLP data-in-motion protection for financial information moving to the cloud.

D. Do not utilize the CASB solution for this purpose, but add DLP on premises for data at rest.

Correct Answer: C

"CASB solutions generally offer their own DLP policy engine, allowing you to configure DLP policies in a CASB and apply them to cloud services."

https://www.mcafee.com/blogs/enterprise/cloud-security/how-a-casb-integrates-with-an-on- premises-dlp- solution/