

KillTest

Higher Quality, Better Service!



Q&A

<http://www.killtest.com>

We offer free update service for one year.

Exam : **CS0-002**

Title : CompTIA Cybersecurity
Analyst (CySA+)
Certification Exam

Version : DEMO

1.As part of a merger with another organization, a Chief Information Security Officer (CISO) is working with an assessor to perform a risk assessment focused on data privacy compliance. The CISO is primarily concerned with the potential legal liability and fines associated with data privacy.

Based on the CISO's concerns, the assessor will MOST likely focus on:

- A. qualitative probabilities.
- B. quantitative probabilities.
- C. qualitative magnitude.
- D. quantitative magnitude.

Answer: D

2.A security analyst reviews the following aggregated output from an Nmap scan and the border firewall ACL:

Server1	Server2	PC1	PC2
22/tcp open	3389/tcp open	80/tcp open	80/tcp open
80/tcp open	53/udp open	443/tcp open	443/tcp open
443/tcp open			1433/tcp open

Firewall ACL

```
10 permit tcp from:any to:server1:www
15 permit udp from:lan-net to:any:dns
16 permit udp from:any to:server2:dns
20 permit tcp from:any to server1:ssl
25 permit tcp from:lan-net to:any:www
26 permit tcp from:lan-net to:any:ssl
27 permit tcp from:any to pc2:mssql
30 permit tcp from:any to server1:ssh
100 deny ip any any
```

Which of the following should the analyst reconfigure to BEST reduce organizational risk while maintaining current functionality?

- A. PC1
- B. PC2
- C. Server1
- D. Server2
- E. Firewall

Answer: B

3.An employee in the billing department accidentally sent a spreadsheet containing payment card data to a recipient outside the organization. The employee intended to send the spreadsheet to an internal staff member with a similar name and was unaware of the mistake until the recipient replied to the message. In addition to retraining the employee, which of the following would prevent this from happening in the future?

- A. Implement outgoing filter rules to quarantine messages that contain card data
- B. Configure the outgoing mail filter to allow attachments only to addresses on the whitelist

- C. Remove all external recipients from the employee's address book
- D. Set the outgoing mail filter to strip spreadsheet attachments from all messages.

Answer: B

4.A new on-premises application server was recently installed on the network. Remote access to the server was enabled for vendor support on required ports, but recent security reports show large amounts of data are being sent to various unauthorized networks through those ports.

Which of the following configuration changes must be implemented to resolve this security issue while still allowing remote vendor access?

- A. Apply a firewall application server rule.
- B. Whitelist the application server.
- C. Sandbox the application server.
- D. Enable port security.
- E. Block the unauthorized networks.

Answer: B

5.A SIEM solution alerts a security analyst of a high number of login attempts against the company's webmail portal. The analyst determines the login attempts used credentials from a past data breach.

Which of the following is the BEST mitigation to prevent unauthorized access?

- A. Single sign-on
- B. Mandatory access control
- C. Multifactor authentication
- D. Federation
- E. Privileged access management

Answer: C