



Free Questions for DES-9131 by actualtestdumps

Shared by Johns on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

The network security team in your company has discovered a threat that leaked partial data on a compromised file server that handles sensitive information. Containment must be initiated and addresses by the CSIRT.

Service disruption is not a concern because this server is used only to store files and does not hold any critical workload. Your company security policy required that all forensic information must be preserved.

Which actions should you take to stop data leakage and comply with requirements of the company security policy?

Options:

- A-** Disconnect the file server from the network to stop data leakage and keep it powered on for further analysis.
- B-** Shut down the server to stop the data leakage and power it up only for further forensic analysis.
- C-** Restart the server to purge all malicious connections and keep it powered on for further analysis.
- D-** Create a firewall rule to block all external connections for this file server and keep it powered on for further analysis.

Answer:

C

Question 2

Question Type: MultipleChoice

What defines who is accountable for contacting operational teams, managers, and others affected by a localized, safety critical event?

Options:

- A- Asset Management Plan
- B- Business Impact Analysis
- C- Business Continuity Plan
- D- Incident Response Plan

Answer:

D

Question 3

Question Type: MultipleChoice

What common process conducted by organizations when protecting digital assets is outside the scope of the NIST Cybersecurity Framework?

Options:

- A- Recover
- B- Identify
- C- Protect
- D- Investigate

Answer:

D

Explanation:

<https://1path.com/blog/overview-of-the-nist-cybersecurity-framework/>

Question 4

Question Type: MultipleChoice

What is the purpose of separation of duties?

Options:

- A- Internal control to prevent fraud
- B- Enhance exposure to functional areas
- C- Encourage collaboration
- D- Mitigate collusion and prevent theft

Answer:

A

Explanation:

<https://www.marsdd.com/mars-library/internal-controls-accounting-key-benefits/>

Question 5

Question Type: MultipleChoice

A continuously updated CMDB is an output of which NIST function and category?

Options:

A- ID.RM

B- ID.SC

C- ID.BE

D- ID.AM

Answer:

A

Question 6

Question Type: MultipleChoice

A new employee is starting work at your company. When should they be informed of the company's security policy?

Options:

- A- Based on human resource policy
- B- After the first security infraction
- C- Annual security policy review
- D- During regular security awareness sessions

Answer:

D

Question 7

Question Type: MultipleChoice

An incident has occurred. You restore backups onto mission/business critical assets. After restoration of the backups your services are still inaccessible on numerous assets.

What could be the cause of the issue?

Options:

- A- Unverified backups
- B- Incorrect backup strategy
- C- Hardware failure
- D- Network failure

Answer:

B

Question 8

Question Type: MultipleChoice

What must be done before returning a compromised laptop to normal operations in the environment?

Options:

- A- Perform a virus scan
- B- Eliminate the root cause of the compromise
- C- Re-image the device
- D- Device cannot be returned to the environment

Answer:

C

Question 9

Question Type: MultipleChoice

The Backup Recovery Plan is dependent on what effort?

Options:

- A- PR.DS
- B- RTO
- C- BIA

D- SDLC

Reference <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-34r1.pdf>

Answer:

B

Question 10

Question Type: MultipleChoice

Which NIST Cybersecurity Framework category ensures that organizational communication and data flows are mapped?

Options:

A- ID.AM

B- ID.GV

C- ID.RA

D- ID.SC

Reference <https://1path.com/blog/overview-of-the-nist-cybersecurity-framework/>

Answer:

A

Question 11

Question Type: MultipleChoice

What are the five functions of the NIST Framework Core?

Options:

A- Identify, Protect, Detect, Respond, and Recover

B- Governance, Identify, Recover, Respond, and Recover

C- Protect, Detect, Respond, Governance, and Recover

D- Identify, Respond, Protect, Detect, and Governance

Reference <https://www.nist.gov/cyberframework/online-learning/five-functions>

Answer:

A

Question 12

Question Type: MultipleChoice

What is considered outside the scope of a BIA?

Options:

- A- Estimated probability of the identified threats actually occurring
- B- Selection of full, incremental, or differential backups
- C- Efficiency and effectiveness of existing risk mitigation controls
- D- Determination of capacity requirements for backups

Answer:

B

To Get Premium Files for DES-9131 Visit

<https://www.p2pexams.com/products/des-9131>

For More Free Questions Visit

<https://www.p2pexams.com/dell-emc/pdf/des-9131>

