Free Questions for CFR-410 by dumpssheet

Shared by Mejia on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following security best practices should a web developer reference when developing a new web- based application?

Options:

A- Control Objectives for Information and Related Technology (COBIT)

B- Risk Management Framework (RMF)

C- World Wide Web Consortium (W3C)

D- Open Web Application Security Project (OWASP)

Answer:

D

Question 2

Question Type: MultipleChoice

Which of the following could be useful to an organization that wants to test its incident response procedures without risking any system downtime?

Options:

A- Blue team exercise

B- Business continuity exercise

C- Tabletop exercise

D- Red team exercise

Answer:

B

Question 3

Question Type: **MultipleChoice**

Which of the following are well-known methods that are used to protect evidence during the forensics process? (Choose three.)

Options:

A- Evidence bags

B- Lock box

C- Caution tape

D- Security envelope

E- Secure rooms

F- Faraday boxes

Answer:

A, C, D

Question 4

Question Type: MultipleChoice

A company help desk is flooded with calls regarding systems experiencing slow performance and certain Internet sites taking a long time to load or not loading at all. The security operations center (SOC) analysts who receive these calls take the following actions:

- Running antivirus scans on the affected user machines

- Checking department membership of affected users

- Checking the host-based intrusion prevention system (HIPS) console for affected user machine alerts

- Checking network monitoring tools for anomalous activities

Which of the following phases of the incident response process match the actions taken?

Options:

A- Identification

B- Preparation

C- Recovery

D- Containment

Answer:

A

Question 5

Question Type: **MultipleChoice**

According to Payment Card Industry Data Security Standard (PCI DSS) compliance requirements, an organization must retain logs for what length of time?

Options:

A- 3 months

B- 6 months

C- 1 year

D- 5 years

Answer:

C

Question 6

Question Type: **MultipleChoice**

During an incident, the following actions have been taken:

- Executing the malware in a sandbox environment

- Reverse engineering the malware

- Conducting a behavior analysis

Based on the steps presented, which of the following incident handling processes has been taken?

Options:

A- Containment

B- Eradication

C- Recovery

D- Identification

Answer:

A

Explanation:

The ''Containment, eradication and recovery'' phase is the period in which incident response team tries to contain the incident and, if necessary, recover from it (restore any affected resources, data and/or processes).

Question 7

Question Type: **MultipleChoice**

An incident handler is assigned to initiate an incident response for a complex network that has been affected by malware. Which of the following actions should be taken FIRST?

Options:

A- Make an incident response plan.

B- Prepare incident response tools.

C- Isolate devices from the network.

D- Capture network traffic for analysis.

Answer:

D

To Get Premium Files for CFR-410 Visit

https://www.p2pexams.com/products/cfr-410

For More Free Questions Visit

https://www.p2pexams.com/certnexus/pdf/cfr-410