GIAC
GCIL
GIAC Cyber Incident Leader (GCIL)

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 6.0

Question: 1

Which practice helps strengthen an incident response team?
Response:

A. Conducting regular training and simulation exercises
B. Waiting for an actual incident before training team members
C. Assigning security responsibilities only to IT staff
D. Focusing only on external threats while ignoring internal risks

Answer: A

Question: 2

Which is a real-world example of a supply chain attack?
Response:

A. SolarWinds breach
B. A phishing attack against an executive
C. A Distributed Denial-of-Service (DDoS) attack on a website
D. A brute-force attack on an employee's account

Answer: A

Question: 3

Which of the following best describes a credential stuffing attack?
Response:

A. A brute-force attack that generates new passwords
B. Using stolen credentials from data breaches to gain unauthorized access
C. Intercepting credentials in transit using a packet sniffer
D. Exploiting a system vulnerability to escalate privileges

Answer: B

Question: 4

Which of the following security measures helps detect and block phishing emails?
Response:

A. Enabling email encryption
B. Configuring email forwarding rules
C. Implementing SPF, DKIM, and DMARC
D. Disabling email filtering

Answer: C

Question: 5

Which stakeholders are typically notified during the incident reporting process?
(Select two.)
Response:

A. Executive leadership
B. Cybercriminals responsible for the attack
C. Regulatory agencies
D. Anonymous online forums

Answer: A,C

Question: 6

Which best practices help improve an organization's vulnerability management process?
(Select two.)
Response:

A. Regularly conducting vulnerability scans
B. Prioritizing vulnerabilities based on risk and exploitability
C. Ignoring low-severity vulnerabilities
D. Only applying patches once per year

Answer: A,B

Question: 7

What are common consequences of a successful email attack?
(Select two.)
Response:

A. Unauthorized access to internal systems
B. Increased email storage capacity
C. Email service performance improvement
D. Financial fraud or data theft

Answer: A,D

Question: 8

What is the primary goal of incident remediation in cybersecurity?
Response:

A. To analyze and document the incident but take no further action
B. To remove the threat, recover affected systems, and prevent recurrence
C. To completely shut down the organization's network after an attack
D. To inform only executive leadership and ignore technical teams

Answer: B

Question: 9

An organization recently experienced a data breach caused by an unpatched software vulnerability. After mitigating the attack, what should they do next to prevent similar incidents?
Response:

A. Conduct a post-incident review, update security policies, and apply patches
B. Ignore the incident since it has been contained
C. Keep using the vulnerable software to study further attacks
D. Avoid informing stakeholders to prevent reputational damage

Answer: A

Question: 10

Your company discovers that a trusted software provider was compromised, and its recent update included malware. What should be your first step?
Response:

A. Isolate affected systems and block the software's network access
B. Ignore the threat since it came from a trusted vendor
C. Publicly accuse the vendor without investigating

D. Pay ransom demands to the attackers

Answer: A

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/