CERTSWARRIOR

GIAC
GCIL
GIAC Cyber Incident Leader (GCIL)

Questions&AnswersPDF

ForMoreInformation:
https://www.certswarrior.com/

Features:

- 90DaysFreeUpdates
- 30DaysMoneyBackGuarantee
- InstantDownloadOncePurchased
- 24/7OnlineChat Support
- ItsLatestVersion

Latest Version: 6.0

Question: 1

Why are supply chain attacks difficult to detect?
Response:

A. They always target physical goods instead of software
B. They only affect large corporations
C. They exploit trusted third-party relationships
D. They require extensive insider knowledge

Answer: C

Question: 2

A financial institution experiences a data breach affecting customer dat
a. Which of the following steps should be taken in the incident reporting process?
Response:
A. Keep the breach secret to avoid reputational damage
B. Notify the affected customers and regulatory authorities
C. Delete all logs related to the breach
D. Fire the security team immediately

Answer: B

Question: 3

Your organization experiences a ransomware attack that encrypts critical files. What should be the immediate response?
Response:

A. Disconnect infected systems from the network
B. Contact the attackers and negotiate the ransom
C. Erase all data without assessing the attack impact
D. Immediately pay the ransom to restore access

Answer: A

Question: 4

Why is incident tracking important in cybersecurity?
Response:

A. It ensures that incidents are resolved efficiently and properly documented
B. It helps companies avoid paying for security tools
C. It allows companies to blame individuals for security failures
D. It removes the need for security teams

Answer: A

Question: 5

Which strategies help mitigate credential-based attacks?
(Select two.)
Response:

A. Enforcing password complexity requirements
B. Implementing passwordless authentication methods
C. Using VPNs to encrypt traffic
D. Blocking all failed login attempts

Answer: A, B

Question: 6

What is the main objective of incident preparation?
Response:

A. Reacting to incidents as they occur
B. Establishing proactive strategies to detect, respond to, and mitigate incidents
C. Ignoring minor security threats
D. Reducing IT security budgets

Answer: B

Question: 7

What is a supply chain attack in cybersecurity?

Response:

A. An attack that exploits only physical supply chains
B. An attack targeting only logistics and transportation companies
C. A social engineering tactic used to steal employee credentials
D. A cyberattack targeting third-party vendors or service providers to compromise their clients

Answer: D

Question: 8

An organization wants to improve its incident tracking system. Which of the following actions would be most effective?
Response:

A. Implementing a ticketing system that tracks status and resolution details
B. Keeping incident logs in unstructured text files
C. Avoiding documentation to minimize effort
D. Relying on employees' memory to recall past incidents

Answer: A

Question: 9

Which best practices enhance incident tracking?
(Select two.)
Response:

A. Maintaining accurate and detailed records
B. Reviewing past incident data for improvements
C. Ignoring minor security alerts
D. Disabling tracking features to reduce costs

Answer: A,B

Question: 10

During an incident assessment, what key questions should be asked to determine the potential risk to an organization?
(Select two.)
Response:

A. What type of data was compromised?
B. What time of day did the attack occur?
C. What vulnerabilities were exploited?
D. How many users were logged in at the time of the attack?

Answer: A,C

CERTSWARRIOR

FULL PRODUCT INCLUDES:

Money Back Guarantee

Instant Download after Purchase

90 Days Free Updates

PDF Format Digital Download

24/7 Live Chat Support

Latest Syllabus Updates

For More Information – Visit link below:

https://www.certswarrior.com

16 USD Discount Coupon Code: U89DY2AQ