212-89 Q&As

EC-Council Certified Incident Handler

Pass EC-COUNCIL 212-89 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/212-89.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Policies are designed to protect the organizational resources on the network by establishing the set rules and procedures. Which of the following policies authorizes a group of users to perform a set of actions on a set of resources?

A. Access control policy

B. Audit trail policy

C. Logging policy

D. Documentation policy

Correct Answer: A

QUESTION 2

One of the goals of CSIRT is to manage security problems by taking a certain approach towards the customers\\' security vulnerabilities and by responding effectively to potential information security incidents. Identify the incident response approach that focuses on developing the infrastructure and security processes before the occurrence or detection of an event or any incident:

A. Interactive approach

B. Introductive approach

C. Proactive approach

D. Qualitative approach

Correct Answer: C

QUESTION 3

Bit stream image copy of the digital evidence must be performed in order to:

A. Prevent alteration to the original disk

B. Copy the FAT table

C. Copy all disk sectors including slack space

D. All the above

Correct Answer: C

QUESTION 4

Which policy recommends controls for securing and tracking organizational resources:

A. Access control policy

B. Administrative security policy

C. Acceptable use policy

D. Asset control policy

Correct Answer: D

QUESTION 5

Which of the following service(s) is provided by the CSIRT:

A. Vulnerability handling

B. Technology watch

C. Development of security tools

D. All the above

Correct Answer: D