Demo Questions

ECOUNCIL 212-89 Exam

EC-Council Certified Incident Handler

Thank you for downloading 212-89 Exam PDF

Question #1 *Topic 1*

Which of the following terms may be defined as "a measure of possible inability to achieve a goal, objective, or target within a defined security, cost plan and technical limitations that adversely affects the organization's operation and revenues?

- A. Risk
- B. Vulnerability
- C. Threat
- D. Incident Response

Correct Answer: *A*

Question #2 *Topic 1*

A distributed Denial of Service (DDoS) attack is a more common type of DoS Attack, where a single system is targeted by a large number of infected machines over the Internet. In a DDoS attack, attackers first infect multiple systems which are known as:

- A. Trojans
- B. Zombies

- C. Spyware
- D. Worms

Correct Answer: *B*

Question #3 ***Topic 1***

The goal of incident response is to handle the incident in a way that minimizes damage and reduces recovery time and cost. Which of the following does NOT constitute a goal of incident response?

- A. Dealing with human resources department and various employee conflict behaviors.
- B. Using information gathered during incident handling to prepare for handling future incidents in a better way and to provide stronger protection for systems and data.
- C. Helping personal to recover quickly and efficiently from security incidents, minimizing loss or theft and disruption of services.
- D. Dealing properly with legal issues that may arise during incidents.

Correct Answer: *A*

Question #4 ***Topic 1***

An organization faced an information security incident where a disgruntled employee passed sensitive access control information to a competitor. The organization's incident response manager, upon investigation, found that the incident must be handled within a few hours on the same day to maintain business continuity and market competitiveness. How would you categorize such information security incident?

- A. High level incident
- B. Middle level incident
- C. Ultra-High level incident
- D. Low level incident

Correct Answer: *A*

Question #5 ***Topic 1***

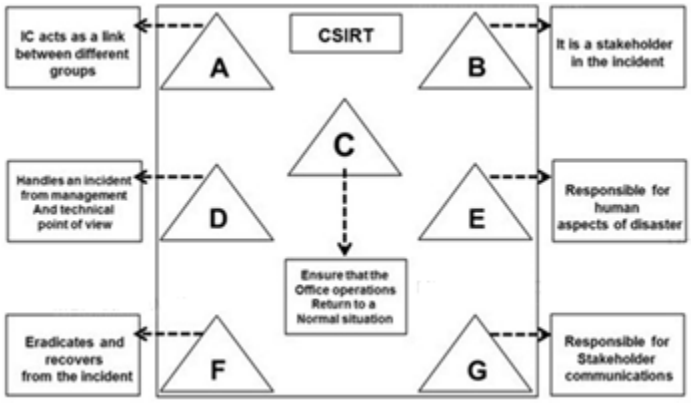
Business continuity is defined as the ability of an organization to continue to function even after a disastrous event, accomplished through the deployment of redundant hardware and software, the use of fault tolerant systems, as well as a solid backup and recovery strategy. Identify the plan which is mandatory part of a business continuity plan?

- A. Forensics Procedure Plan
- B. Business Recovery Plan
- C. Sales and Marketing plan
- D. New business strategy plan

Correct Answer: *B*

Question #6*Topic 1*

The flow chart gives a view of different roles played by the different personnel of CSIRT. Identify the incident response personnel denoted by A, B, C, D, E, F and G.



- A. A-Incident Analyst, B- Incident Coordinator, C- Public Relations, D-Administrator, E-Human Resource, F-Constituency, G-Incident Manager
- B. A- Incident Coordinator, B-Incident Analyst, C- Public Relations, D-Administrator, E-Human Resource, F-Constituency, G-Incident Manager
- C. A- Incident Coordinator, B- Constituency, C-Administrator, D-Incident Manager, E-Human Resource, F-Incident Analyst, G-Public relations
- D. A- Incident Manager, B-Incident Analyst, C- Public Relations, D-Administrator, E-Human Resource, F-Constituency, G-Incident Coordinator

Correct Answer: *C*

Question #7 ***Topic 1***

Which of the following is an appropriate flow of the incident recovery steps?

- A. System Operation-System Restoration-System Validation-System Monitoring
- B. System Validation-System Operation-System Restoration-System Monitoring
- C. System Restoration-System Monitoring-System Validation-System Operations
- D. System Restoration-System Validation-System Operations-System Monitoring

Correct Answer: *D*

Question #8 ***Topic 1***

A computer Risk Policy is a set of ideas to be implemented to overcome the risk associated with computer security incidents. Identify the procedure that is NOT part of the computer risk policy?

- A. Procedure to identify security funds to hedge risk
- B. Procedure to monitor the efficiency of security controls
- C. Procedure for the ongoing training of employees authorized to access the system
- D. Provisions for continuing support if there is an interruption in the system or if the system crashes

Correct Answer: *C*