Eccouncil

212-89 Exam

EC Council Certified Incident Handler (ECIH v2) Exam

Questions & Answers
Demo

Version: 8.0

Question: 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

Answer: A

Question: 2

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

Answer: B

Question: 3

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.

Answer: A

Question: 4

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

Answer: A

Question: 5

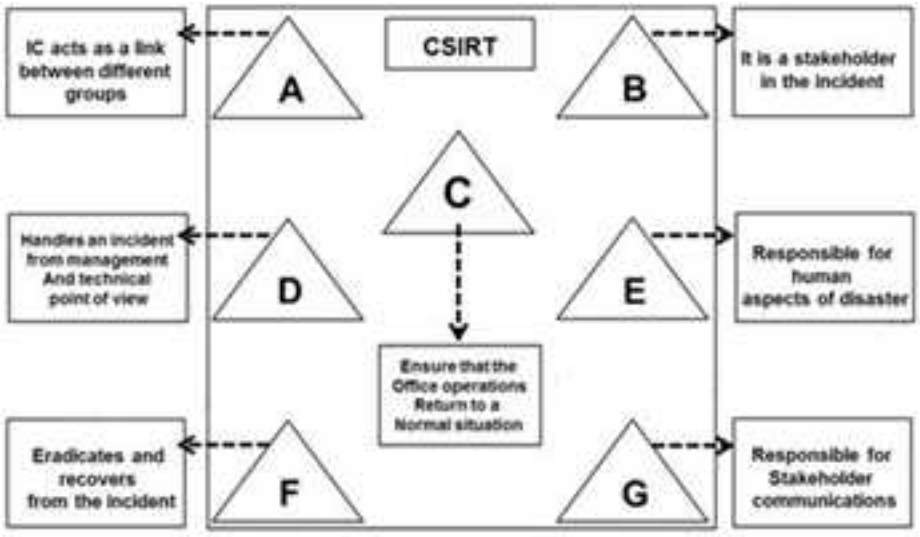
Business continuity is defined as the ability of an organization to continue to function even after a disastrous event, accomplished through the deployment of redundant hardware and software, the use of fault tolerant systems, as well as a solid backup and recovery strategy. Identify the plan which is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

Answer: B

Question: 6

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

Answer: C

Question: 7

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

Answer: D

Question: 8

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

Answer: C

Question: 9

Identify the network security incident where intended authorized users are prevented from using system, network, or applications by flooding the network with high volume of traffic that consumes all existing network resources.

A. URL Manipulation
B. XSS Attack
C. SQL Injection
D. Denial of Service Attack

Answer: D

Question: 10

Incident handling and response steps help you to detect, identify, respond and manage an incident. Which of the following steps focus on limiting the scope and extent of an incident?

A. Eradication
B. Containment
C. Identification
D. Data collection

Answer: B