Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

212-89 Dumps
212-89 Braindumps
212-89 Real Questions
212-89 Practice Test
212-89 Actual Questions

PASS

EC-Council

212-89

EC-Council Certified Incident Handler (ECIH v2)

Question: 153

Quantitative risk is the numerical determination of the probability of an adverse event and the extent of the losses due to the event. Quantitative risk is calculated as:
A. (Probability of Loss) X (Loss)
B. (Loss) / (Probability of Loss)
C. (Probability of Loss) / (Loss)
D. Significant Risks X Probability of Loss X Loss

Answer: A

Question: 154

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

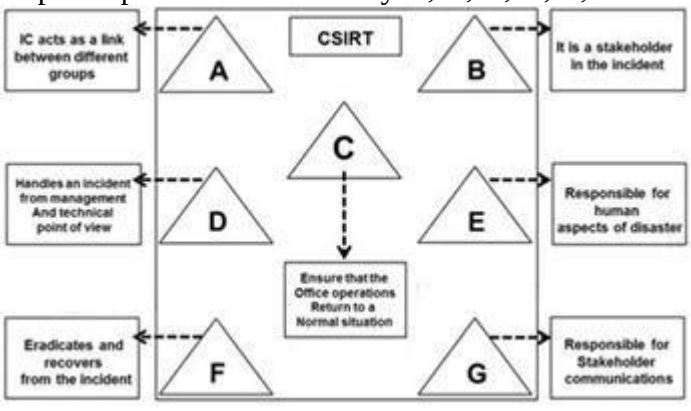
Question: 155

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

Question: 156

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: 157

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: 158

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: 159

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: 160

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: 161

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: 162

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: 163

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

SAMPLE QUESTIONS

These questions are for demo purpose only. ***Full version*** *is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions*: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

Exam Dumps*: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

Practice Tests*: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

Guaranteed Success*: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

Updated Content: *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

Technical Support*: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*