

## Exam Questions 212-89

EC Council Certified Incident Handler (ECIH v2)

<https://www.2passeasy.com/dumps/212-89/>



#### NEW QUESTION 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, FConstituency, G-Incident Manager
- B. A- Incident Coordinator, B-Incident Analyst, C- Public Relations, D-Administrator, E- Human Resource, FConstituency, G-Incident Manager
- C. A- Incident Coordinator, B- Constituency, C-Administrator, D-Incident Manager, E- Human Resource, FIncident Analyst, G-Public relations
- D. A- Incident Manager, B-Incident Analyst, C- Public Relations, D-Administrator, E- Human Resource, FConstituency, G-Incident Coordinator

**Answer: C**

#### NEW QUESTION 2

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**

#### NEW QUESTION 3

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**

#### NEW QUESTION 4

Risk is defined as the probability of the occurrence of an incident. Risk formulation generally begins with the likeliness of an event's occurrence, the harm it may cause and is usually denoted as Risk = ?(events)X (Probability of occurrence)X?

- A. Magnitude
- B. Probability
- C. Consequences
- D. Significance

**Answer:** A

#### NEW QUESTION 5

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

**Answer:** A

#### NEW QUESTION 6

In the Control Analysis stage of the NIST's risk assessment methodology, technical and none technical control methods are classified into two categories. What are these two control categories?

- A. Preventive and Detective controls
- B. Detective and Disguised controls
- C. Predictive and Detective controls
- D. Preventive and predictive controls

**Answer:** A

#### NEW QUESTION 7

The insider risk matrix consists of technical literacy and business process knowledge vectors. Considering the matrix, one can conclude that:

- A. If the insider's technical literacy is low and process knowledge is high, the risk posed by the threat will be insignificant.
- B. If the insider's technical literacy and process knowledge are high, the risk posed by the threat will be insignificant.
- C. If the insider's technical literacy is high and process knowledge is low, the risk posed by the threat will be high.
- D. If the insider's technical literacy and process knowledge are high, the risk posed by the threat will be high.

**Answer:** D

#### NEW QUESTION 8

The data on the affected system must be backed up so that it can be retrieved if it is damaged during incident response. The system backup can also be used for further investigations of the incident. Identify the stage of the incident response and handling process in which complete backup of the infected system is carried out?

- A. Containment
- B. Eradication
- C. Incident recording
- D. Incident investigation

**Answer:** A

#### NEW QUESTION 9

A computer virus hoax is a message warning the recipient of non-existent computer virus. The message is usually a chain e-mail that tells the recipient to forward it to every one they know. Which of the following is NOT a symptom of virus hoax message?

- A. The message prompts the end user to forward it to his / her e-mail contact list and gain monetary benefits in doing so
- B. The message from a known email id is caught by SPAM filters due to change of filter settings
- C. The message warns to delete certain files if the user does not take appropriate action
- D. The message prompts the user to install Anti-Virus

**Answer:** A

#### NEW QUESTION 10

In which of the steps of NIST's risk assessment methodology are the boundary of the IT system, along with the resources and the information that constitute the system identified?

- A. Likelihood Determination
- B. Control recommendation
- C. System characterization
- D. Control analysis

**Answer:** C

#### NEW QUESTION 10

An assault on system security that is derived from an intelligent threat is called:

- A. Threat Agent
- B. Vulnerability
- C. Attack
- D. Risk

**Answer:** C

**NEW QUESTION 11**

Incident prioritization must be based on:

- A. Potential impact
- B. Current damage
- C. Criticality of affected systems
- D. All the above

**Answer:** D

**NEW QUESTION 12**

Which of the following can be considered synonymous:

- A. Hazard and Threat
- B. Threat and Threat Agent
- C. Precaution and countermeasure
- D. Vulnerability and Danger

**Answer:** A

**NEW QUESTION 13**

A payroll system has a vulnerability that cannot be exploited by current technology. Which of the following is correct about this scenario:

- A. The risk must be urgently mitigated
- B. The risk must be transferred immediately
- C. The risk is not present at this time
- D. The risk is accepted

**Answer:** C

**NEW QUESTION 16**

What is correct about Quantitative Risk Analysis:

- A. It is Subjective but faster than Qualitative Risk Analysis
- B. Easily automated
- C. Better than Qualitative Risk Analysis
- D. Uses levels and descriptive expressions

**Answer:** B

**NEW QUESTION 19**

Which of the following is a risk assessment tool:

- A. Nessus
- B. Wireshark
- C. CRAMM
- D. Nmap

**Answer:** C

**NEW QUESTION 23**

Incident Response Plan requires

- A. Financial and Management support
- B. Expert team composition
- C. Resources
- D. All the above

**Answer:** D

**NEW QUESTION 28**

The main feature offered by PGP Desktop Email is:

- A. Email service during incidents
- B. End-to-end email communications
- C. End-to-end secure email service
- D. None of the above

**Answer:** C

**NEW QUESTION 31**

The program that helps to train people to be better prepared to respond to emergency situations in their communities is known as:

- A. Community Emergency Response Team (CERT)
- B. Incident Response Team (IRT)
- C. Security Incident Response Team (SIRT)
- D. All the above

**Answer:** A

#### NEW QUESTION 32

Installing a password cracking tool, downloading pornography material, sending emails to colleagues which irritates them and hosting unauthorized websites on the company's computer are considered:

- A. Network based attacks
- B. Unauthorized access attacks
- C. Malware attacks
- D. Inappropriate usage incidents

**Answer:** D

#### NEW QUESTION 33

To respond to DDoS attacks; one of the following strategies can be used:

- A. Using additional capacity to absorb attack
- B. Identifying none critical services and stopping them
- C. Shut down some services until the attack has subsided
- D. All the above

**Answer:** D

#### NEW QUESTION 34

A malware code that infects computer files, corrupts or deletes the data in them and requires a host file to propagate is called:

- A. Trojan
- B. Worm
- C. Virus
- D. RootKit

**Answer:** C

#### NEW QUESTION 38

A self-replicating malicious code that does not alter files but resides in active memory and duplicates itself, spreads through the infected network automatically and takes advantage of file or information transport features on the system to travel independently is called:

- A. Trojan
- B. Worm
- C. Virus
- D. RootKit

**Answer:** B

#### NEW QUESTION 41

The message that is received and requires an urgent action and it prompts the recipient to delete certain files or forward it to others is called:

- A. An Adware
- B. Mail bomb
- C. A Virus Hoax
- D. Spear Phishing

**Answer:** C

#### NEW QUESTION 46

A software application in which advertising banners are displayed while the program is running that delivers ads to display pop-up windows or bars that appears on a computer screen or browser is called:

- A. adware (spelled all lower case)
- B. Trojan
- C. RootKit
- D. Virus
- E. Worm

**Answer:** A

#### NEW QUESTION 50

Which of the following is NOT one of the techniques used to respond to insider threats:

- A. Placing malicious users in quarantine network, so that attack cannot be spread

- B. Preventing malicious users from accessing unclassified information
- C. Disabling the computer systems from network connection
- D. Blocking malicious user accounts

**Answer:** B

#### NEW QUESTION 54

Insiders understand corporate business functions. What is the correct sequence of activities performed by Insiders to damage company assets:

- A. Gain privileged access, install malware then activate
- B. Install malware, gain privileged access, then activate
- C. Gain privileged access, activate and install malware
- D. Activate malware, gain privileged access then install malware

**Answer:** A

#### NEW QUESTION 57

Which of the following may be considered as insider threat(s):

- A. An employee having no clashes with supervisors and coworkers
- B. Disgruntled system administrators
- C. An employee who gets an annual 7% salary raise
- D. An employee with an insignificant technical literacy and business process knowledge

**Answer:** B

#### NEW QUESTION 60

Lack of forensic readiness may result in:

- A. Loss of clients thereby damaging the organization's reputation
- B. System downtime
- C. Data manipulation, deletion, and theft
- D. All the above

**Answer:** D

#### NEW QUESTION 64

What command does a Digital Forensic Examiner use to display the list of all IP addresses and their associated MAC addresses on a victim computer to identify the machines that were communicating with it:

- A. "arp" command
- B. "netstat -an" command
- C. "dd" command
- D. "ifconfig" command

**Answer:** A

#### NEW QUESTION 66

Incidents are reported in order to:

- A. Provide stronger protection for systems and data
- B. Deal properly with legal issues
- C. Be prepared for handling future incidents
- D. All the above

**Answer:** D

#### NEW QUESTION 68

According to US-CERT; if an agency is unable to successfully mitigate a DOS attack it must be reported within:

- A. One (1) hour of discovery/detection if the successful attack is still ongoing
- B. Two (2) hours of discovery/detection if the successful attack is still ongoing
- C. Three (3) hours of discovery/detection if the successful attack is still ongoing
- D. Four (4) hours of discovery/detection if the successful attack is still ongoing

**Answer:** B

#### NEW QUESTION 69

Agencies do NOT report an information security incident is because of:

- A. Afraid of negative publicity
- B. Have full knowledge about how to handle the attack internally
- C. Do not want to pay the additional cost of reporting an incident
- D. All the above

**Answer:** A

**NEW QUESTION 74**

To whom should an information security incident be reported?

- A. It should not be reported at all and it is better to resolve it internally
- B. Human resources and Legal Department
- C. It should be reported according to the incident reporting & handling policy
- D. Chief Information Security Officer

**Answer:** C

**NEW QUESTION 76**

Business Continuity planning includes other plans such as:

- A. Incident/disaster recovery plan
- B. Business recovery and resumption plans
- C. Contingency plan
- D. All the above

**Answer:** D

**NEW QUESTION 79**

Ensuring the integrity, confidentiality and availability of electronic protected health information of a patient is known as:

- A. Gramm-Leach-Bliley Act
- B. Health Insurance Portability and Privacy Act
- C. Social Security Act
- D. Sarbanes-Oxley Act

**Answer:** B

**NEW QUESTION 81**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 212-89 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 212-89 Product From:

<https://www.2passeasy.com/dumps/212-89/>

## Money Back Guarantee

### 212-89 Practice Exam Features:

- \* 212-89 Questions and Answers Updated Frequently
- \* 212-89 Practice Questions Verified by Expert Senior Certified Staff
- \* 212-89 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* 212-89 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year