

## 212-89 Dumps

### EC Council Certified Incident Handler (ECIH v2)

<https://www.certleader.com/212-89-dumps.html>



**NEW QUESTION 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

**Answer:** D

**NEW QUESTION 2**

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

**NEW QUESTION 3**

Multiple component incidents consist of a combination of two or more attacks in a system. Which of the following is not a multiple component incident?

- A. An insider intentionally deleting files from a workstation
- B. An attacker redirecting user to a malicious website and infects his system with Trojan
- C. An attacker infecting a machine to launch a DDoS attack
- D. An attacker using email with malicious code to infect internal workstation

**Answer:** A

**NEW QUESTION 4**

Computer Forensics is the branch of forensic science in which legal evidence is found in any computer or any digital media device. Of the following, who is responsible for examining the evidence acquired and separating the useful evidence?

- A. Evidence Supervisor
- B. Evidence Documenter
- C. Evidence Manager
- D. Evidence Examiner/ Investigator

**Answer:** D

**NEW QUESTION 5**

When an employee is terminated from his or her job, what should be the next immediate step taken by an organization?

- A. All access rights of the employee to physical locations, networks, systems, applications and data should be disabled
- B. The organization should enforce separation of duties
- C. The access requests granted to an employee should be documented and vetted by the supervisor
- D. The organization should monitor the activities of the system administrators and privileged users who have permissions to access the sensitive information

**Answer:** A

**NEW QUESTION 6**

Which among the following CERTs is an Internet provider to higher education institutions and various other research institutions in the Netherlands and deals with all cases related to computer security incidents in which a customer is involved either as a victim or as a suspect?

- A. NET-CERT
- B. DFN-CERT
- C. Funet CERT
- D. SURFnet-CERT

**Answer:** D

**NEW QUESTION 7**

Contingency planning enables organizations to develop and maintain effective methods to handle emergencies. Every organization will have its own specific requirements that the planning should address. There are five major components of the IT contingency plan, namely supporting information, notification activation, recovery and reconstitution and plan appendices. What is the main purpose of the reconstitution plan?

- A. To restore the original site, tests systems to prevent the incident and terminates operations
- B. To define the notification procedures, damage assessments and offers the plan activation
- C. To provide the introduction and detailed concept of the contingency plan
- D. To provide a sequence of recovery activities with the help of recovery procedures

**Answer:** A

**NEW QUESTION 8**

Except for some common roles, the roles in an IRT are distinct for every organization. Which among the following is the role played by the Incident Coordinator of an IRT?

- A. Links the appropriate technology to the incident to ensure that the foundation's offices are returned to normal operations as quickly as possible
- B. Links the groups that are affected by the incidents, such as legal, human resources, different business areas and management
- C. Applies the appropriate technology and tries to eradicate and recover from the incident
- D. Focuses on the incident and handles it from management and technical point of view

**Answer: B**

**NEW QUESTION 9**

In a qualitative risk analysis, risk is calculated in terms of:

- A. (Attack Success + Criticality ) –(Countermeasures)
- B. Asset criticality assessment – (Risks and Associated Risk Levels)
- C. Probability of Loss X Loss
- D. (Countermeasures + Magnitude of Impact) – (Reports from prior risk assessments)

**Answer: C**

**NEW QUESTION 10**

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**

ADAM, an employee from a multinational company, uses his company's accounts to send e-mails to a third party with their spoofed mail address. How can you categorize this type of account?

- A. Inappropriate usage incident
- B. Unauthorized access incident
- C. Network intrusion incident
- D. Denial of Service incident

**Answer: A**

**NEW QUESTION 15**

Incident handling and response steps help you to detect, identify, respond and manage an incident. Which of the following helps in recognizing and separating the infected hosts from the information system?

- A. Configuring firewall to default settings
- B. Inspecting the process running on the system
- C. Browsing particular government websites
- D. Sending mails to only group of friends

**Answer: B**

**NEW QUESTION 18**

An estimation of the expected losses after an incident helps organization in prioritizing and formulating their incident response. The cost of an incident can be categorized as a tangible and intangible cost. Identify the tangible cost associated with virus outbreak?

- A. Loss of goodwill
- B. Damage to corporate reputation
- C. Psychological damage
- D. Lost productivity damage

**Answer: D**

**NEW QUESTION 21**

A risk mitigation strategy determines the circumstances under which an action has to be taken to minimize and overcome risks. Identify the risk mitigation strategy that focuses on minimizing the probability of risk and losses by searching for vulnerabilities in the system and appropriate controls:

- A. Risk Assumption
- B. Research and acknowledgment
- C. Risk limitation
- D. Risk absorption

**Answer: B**

**NEW QUESTION 23**

Based on the some statistics; what is the typical number one top incident?

- A. Phishing
- B. Policy violation
- C. Un-authorized access
- D. Malware

**Answer:** A

**NEW QUESTION 26**

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 28**

Incidents such as DDoS that should be handled immediately may be considered as:

- A. Level One incident
- B. Level Two incident
- C. Level Three incident
- D. Level Four incident

**Answer:** C

**NEW QUESTION 29**

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 34**

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 36**

If the loss anticipated is greater than the agreed upon threshold; the organization will:

- A. Accept the risk
- B. Mitigate the risk
- C. Accept the risk but after management approval
- D. Do nothing

**Answer:** B

**NEW QUESTION 38**

Overall Likelihood rating of a Threat to Exploit a Vulnerability is driven by :

- A. Threat-source motivation and capability
- B. Nature of the vulnerability
- C. Existence and effectiveness of the current controls
- D. All the above

**Answer:** D

**NEW QUESTION 39**

Removing or eliminating the root cause of the incident is called:

- A. Incident Eradication

- B. Incident Protection
- C. Incident Containment
- D. Incident Classification

**Answer:** A

**NEW QUESTION 43**

Incident Response Plan requires

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

**Answer:** D

**NEW QUESTION 45**

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

**Answer:** D

**NEW QUESTION 49**

The free, open source, TCP/IP protocol analyzer, sniffer and packet capturing utility standard across many industries and educational institutions is known as:

- A. Snort
- B. Wireshark
- C. Cain & Able
- D. nmap

**Answer:** B

**NEW QUESTION 54**

The very well-known free open source port, OS and service scanner and network discovery utility is called:

- A. Wireshark
- B. Nmap (Network Mapper)
- C. Snort
- D. SAINT

**Answer:** B

**NEW QUESTION 59**

A malicious security-breaking code that is disguised as any useful program that installs an executable programs when a file is opened and allows others to control the victim's system is called:

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

**Answer:** A

**NEW QUESTION 60**

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 65**

The free utility which quickly scans Systems running Windows OS to find settings that may have been changed by spyware, malware, or other unwanted programs is called:

- A. Tripwire
- B. HijackThis
- C. Stinger
- D. F-Secure Anti-virus

**Answer:** B

**NEW QUESTION 69**

The main difference between viruses and worms is:

- A. Worms require a host file to propagate while viruses don't
- B. Viruses require a host file to propagate while Worms don't
- C. Viruses don't require user interaction; they are self-replicating malware
- D. Viruses and worms are common names for the same malware

**Answer:** B

**NEW QUESTION 72**

The sign(s) of the presence of malicious code on a host infected by a virus which is delivered via e-mail could be:

- A. Antivirus software detects the infected files
- B. Increase in the number of e-mails sent and received
- C. System files become inaccessible
- D. All the above

**Answer:** D

**NEW QUESTION 76**

Spyware tool used to record malicious user's computer activities and keyboard strokes is called:

- A. adware
- B. Keylogger
- C. Rootkit
- D. Firewall

**Answer:** B

**NEW QUESTION 77**

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 79**

Which of the following is NOT a digital forensic analysis tool:

- A. Access Data FTK
- B. EAR/ Pilar
- C. Guidance Software EnCase Forensic
- D. Helix

**Answer:** B

**NEW QUESTION 80**

What command does a Digital Forensic Examiner use to display the list of all open ports and the associated IP addresses on a victim computer to identify the established connections on it:

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

**Answer:** B

**NEW QUESTION 84**

Digital evidence must:

- A. Be Authentic, complete and reliable
- B. Not prove the attackers actions
- C. Be Volatile
- D. Cast doubt on the authenticity and veracity of the evidence

**Answer:** A

**NEW QUESTION 85**

The process of rebuilding and restoring the computer systems affected by an incident to normal operational stage including all the processes, policies and tools is known as:

- A. Incident Management
- B. Incident Response
- C. Incident Recovery
- D. Incident Handling

**Answer:** C

**NEW QUESTION 90**

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 92**

The ability of an agency 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 is known as:

- A. Business Continuity Plan
- B. Business Continuity
- C. Disaster Planning
- D. Contingency Planning

**Answer:** B

**NEW QUESTION 97**

The policy that defines which set of events needs to be logged in order to capture and review the important data in a timely manner is known as:

- A. Audit trail policy
  - B. Logging policy
  - C. Documentation policy
  - D. Evidence Collection policy
  - E. Distributed and communicated
  - F. Enforceable and Regularly updated
  - G. Written in simple language
  - H. All the above
- An information security policy must be:

**Answer:** D

**NEW QUESTION 100**

According to the Evidence Preservation policy, a forensic investigator should make at least ..... image copies of the digital evidence.

- A. One image copy
- B. Two image copies
- C. Three image copies
- D. Four image copies

**Answer:** B

**NEW QUESTION 101**

.....



## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your 212-89 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/212-89-dumps.html>