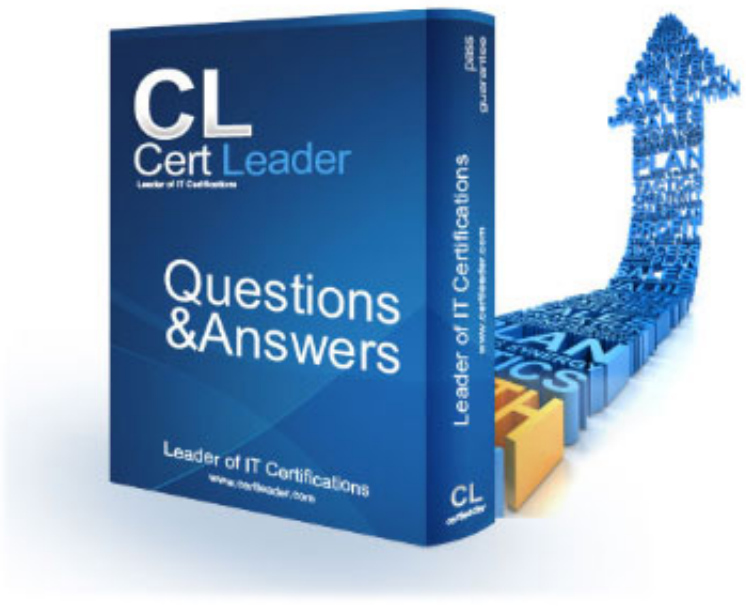
# 212-89 Dumps

# EC Council Certified Incident Handler (ECIH v2)

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



**NEW QUESTION 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

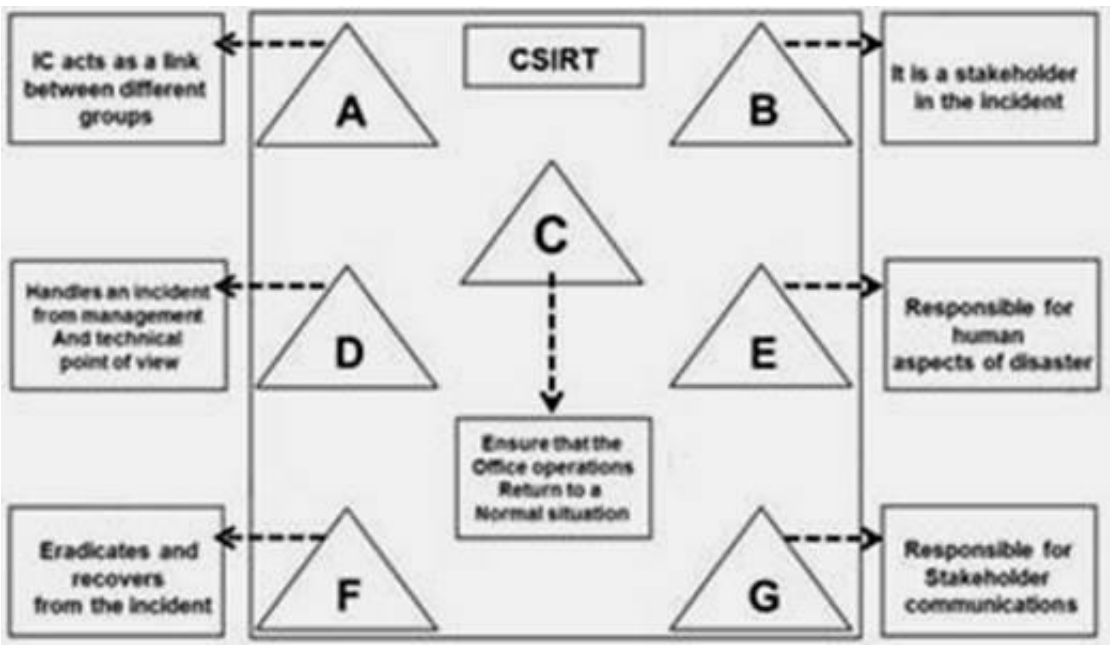
**Answer:** B

**NEW QUESTION 2**
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

**NEW QUESTION 3**
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 4**
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

**NEW QUESTION 5**
Identify the malicious program that is masked as a genuine harmless program and gives the attacker unrestricted access to the user's information and system. These programs may unleash dangerous programs that may erase the unsuspecting user's disk and send the victim's credit card numbers and passwords to a stranger.

A. Cookie tracker
B. Worm
C. Trojan
D. Virus

**Answer:** C

**NEW QUESTION 6**
An audit trail policy collects all audit trails such as series of records of computer events, about an operating system, application or user activities. Which of the following statements is NOT true for an audit trail policy:

A. It helps calculating intangible losses to the organization due to incident
B. It helps tracking individual actions and allows users to be personally accountable for their actions
C. It helps in compliance to various regulatory laws, rules,and guidelines
D. It helps in reconstructing the events after a problem has occurred

**Answer:** A

**NEW QUESTION 7**
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 8**
The network perimeter should be configured in such a way that it denies all incoming and outgoing traffic/ services that are not required. Which service listed below, if blocked, can help in preventing Denial of Service attack?

A. SAM service
B. POP3 service
C. SMTP service
D. Echo service

**Answer:** D

**NEW QUESTION 9**
US-CERT and Federal civilian agencies use the reporting timeframe criteria in the federal agency reporting categorization. What is the timeframe required to report an incident under the CAT 4 Federal Agency category?

A. Weekly
B. Within four (4) hours of discovery/detection if the successful attack is still ongoing and agency is unable to successfully mitigate activity
C. Within two (2) hours of discovery/detection
D. Monthly

**Answer:** A

**NEW QUESTION 10**
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 10**
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 14**
An incident is analyzed for its nature, intensity and its effects on the network and systems. Which stage of the incident response and handling process involves auditing the system and network log files?

A. Incident recording
B. Reporting
C. Containment
D. Identification

**Answer:** D

**NEW QUESTION 16**
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 18**
Insider threats can be detected by observing concerning behaviors exhibited by insiders, such as conflicts with supervisors and coworkers, decline in performance, tardiness or unexplained absenteeism. Select the technique that helps in detecting insider threats:

A. Correlating known patterns of suspicious and malicious behavior
B. Protecting computer systems by implementing proper controls
C. Making is compulsory for employees to sign a none disclosure agreement
D. Categorizing information according to its sensitivity and access rights

**Answer:** A

**NEW QUESTION 21**
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 22**
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 27**
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 29**
An access control policy authorized a group of users to perform a set of actions on a set of resources. Access to resources is based on necessity and if a particular job role requires the use of those resources. Which of the following is NOT a fundamental element of access control policy

A. Action group: group of actions performed by the users on resources
B. Development group: group of persons who develop the policy
C. Resource group: resources controlled by the policy
D. Access group: group of users to which the policy applies

**Answer:** B

**NEW QUESTION 31**
Digital evidence plays a major role in prosecuting cyber criminals. John is a cyber-crime investigator, is asked to investigate a child pornography case. The personal computer of the criminal in question was confiscated by the county police. Which of the following evidence will lead John in his investigation?

A. SAM file
B. Web serve log
C. Routing table list
D. Web browser history

**Answer:**

D

**NEW QUESTION 35**
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 36**
Which of the following incidents are reported under CAT -5 federal agency category?

A. Exercise/ Network Defense Testing
B. Malicious code
C. Scans/ probes/ Attempted Access
D. Denial of Service DoS

**Answer:** C

**NEW QUESTION 38**
One of the goals of CSIRT is to manage security problems by taking a certain approach towards the customers' security vulnerabilities and by responding effectively to potential information security incidents. Identify the incident response approach that focuses on developing the infrastructure and security processes before the occurrence or detection of an event or any incident:

A. Interactive approach
B. Introductive approach
C. Proactive approach
D. Qualitative approach

**Answer:** C

**NEW QUESTION 39**
Incident management team provides support to all users in the organization that are affected by the threat or attack. The organization's internal auditor is part of the incident response team. Identify one of the responsibilities of the internal auditor as part of the incident response team:

A. Configure information security controls
B. Perform necessary action to block the network traffic from suspected intruder
C. Identify and report security loopholes to the management for necessary actions
D. Coordinate incident containment activities with the information security officer

**Answer:** C

**NEW QUESTION 40**
An adversary attacks the information resources to gain undue advantage is called:

A. Defensive Information Warfare
B. Offensive Information Warfare
C. Electronic Warfare
D. Conventional Warfare

**Answer:** B

**NEW QUESTION 44**
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 47**
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 52**
Total cost of disruption of an incident is the sum of

A. Tangible and Intangible costs
B. Tangible cost only
C. Intangible cost only
D. Level Two and Level Three incidents cost

**Answer:** A

**NEW QUESTION 53**
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 57**
An information security incident is

A. Any real or suspected adverse event in relation to the security of computer systems or networks
B. Any event that disrupts normal today's business functions
C. Any event that breaches the availability of information assets
D. All of the above

**Answer:** D

**NEW QUESTION 61**
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 65**
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 70**
Absorbing minor risks while preparing to respond to major ones is called:

A. Risk Mitigation
B. Risk Transfer
C. Risk Assumption
D. Risk Avoidance

**Answer:** C

**NEW QUESTION 74**
Adam calculated the total cost of a control to protect 10,000 $ worth of data as 20,000 $. What do you advise Adam to do?

A. Apply the control
B. Not to apply the control
C. Use qualitative risk assessment
D. Use semi-qualitative risk assessment instead

**Answer:** B

**NEW QUESTION 77**
Which of the following is a risk assessment tool:

A. Nessus

B. Wireshark
C. CRAMM
D. Nmap

**Answer:** C

**NEW QUESTION 78**
The correct sequence of incident management process is:

A. Prepare, protect, triage, detect and respond
B. Prepare, protect, detect, triage and respond
C. Prepare, detect, protect, triage and respond
D. Prepare, protect, detect, respond and triage

**Answer:** B

**NEW QUESTION 82**
Incident response team must adhere to the following:

A. Stay calm and document everything
B. Assess the situation
C. Notify appropriate personnel
D. All the above

**Answer:** D

**NEW QUESTION 84**
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 87**
Which of the following is a correct statement about incident management, handling and response:

A. Incident response is on the functions provided by incident handling
B. Incident handling is on the functions provided by incident response
C. Triage is one of the services provided by incident response
D. Incident response is one of the services provided by triage

**Answer:** A

**NEW QUESTION 89**
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 92**
CERT members can provide critical support services to first responders such as:

A. Immediate assistance to victims
B. Consolidated automated service process management platform
C. Organizing spontaneous volunteers at a disaster site
D. A + C

**Answer:** D

**NEW QUESTION 95**
The region where the CSIRT is bound to serve and what does it and give service to is known as:

A. Consistency
B. Confidentiality
C. Constituency
D. None of the above

**Answer:** C

**NEW QUESTION 99**
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 104**
CSIRT can be implemented at:

A. Internal enterprise level
B. National, government and military level
C. Vendor level
D. All the above

**Answer:** D

**NEW QUESTION 109**
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 111**
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 115**
They type of attack that prevents the authorized users to access networks, systems, or applications by exhausting the network resources and sending illegal requests to an application is known as:

A. Session Hijacking attack
B. Denial of Service attack
C. Man in the Middle attack
D. SQL injection attack

**Answer:** B

**NEW QUESTION 120**
_____ record(s) user's typing.

A. Spyware
B. adware
C. Virus
D. Malware

**Answer:** A

**NEW QUESTION 121**
Which of the following is a characteristic of adware?

A. Gathering information
B. Displaying popups
C. Intimidating users
D. Replicating

**Answer:** B

**NEW QUESTION 123**
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 125**
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 130**
Authorized users with privileged access who misuse the corporate informational assets and directly affects the confidentiality, integrity, and availability of the assets are known as:

A. Outsider threats
B. Social Engineers
C. Insider threats
D. Zombies

**Answer:** C

**NEW QUESTION 131**
The USB tool (depicted below) that is connected to male USB Keyboard cable and not detected by antispyware tools is most likely called:

A. Software Key Grabber
B. Hardware Keylogger
C. USB adapter
D. Anti-Keylogger

**Answer:** B

**NEW QUESTION 136**
Insiders may be:

A. Ignorant employees
B. Carless administrators
C. Disgruntled staff members
D. All the above

**Answer:** D

**NEW QUESTION 139**
The state of incident response preparedness that enables an organization to maximize its potential to use digital evidence while minimizing the cost of an investigation is called:

A. Computer Forensics
B. Digital Forensic Analysis
C. Forensic Readiness
D. Digital Forensic Policy

**Answer:** C

**NEW QUESTION 140**
The Linux command used to make binary copies of computer media and as a disk imaging tool if given a raw disk device as its input is:

A. "dd" command

B. “netstat” command
C. “nslookup” command
D. “find” command

**Answer:** A

**NEW QUESTION 142**
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 146**
The individual who recovers, analyzes, and preserves computer and related materials to be presented as evidence in a court of law and identifies the evidence, estimates the potential impact of the malicious activity on the victim, and assesses the intent and identity of the perpetrator is called:

A. Digital Forensic Examiner
B. Computer Forensic Investigator
C. Computer Hacking Forensic Investigator
D. All the above

**Answer:** D

**NEW QUESTION 148**
The person who offers his formal opinion as a testimony about a computer crime incident in the court of law is known as:

A. Expert Witness
B. Incident Analyzer
C. Incident Responder
D. Evidence Documenter

**Answer:** A

**NEW QUESTION 153**
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 156**
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 158**
Business Continuity provides a planning methodology that allows continuity in business operations:

A. Before and after a disaster
B. Before a disaster
C. Before, during and after a disaster
D. During and after a disaster

**Answer:** C

**NEW QUESTION 160**
The product of intellect that has commercial value and includes copyrights and trademarks is called:

A. Intellectual property
B. Trade secrets
C. Logos

D. Patents

**Answer:** A

**NEW QUESTION 162**
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 164**
According to the Fourth Amendment of USA PATRIOT Act of 2001; if a search does NOT violate a person's "reasonable" or "legitimate" expectation of privacy then it is considered:

A. Constitutional/ Legitimate
B. Illegal/ illegitimate
C. Unethical
D. None of the above

**Answer:** A

**NEW QUESTION 166**
A living high level document that states in writing a requirement and directions on how an agency plans to protect its information technology assets is called:

A. Information security Policy
B. Information security Procedure
C. Information security Baseline
D. Information security Standard

**Answer:** A

**NEW QUESTION 169**
.....

# 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