

Exam Questions 212-89

EC Council Certified Incident Handler (ECIH v2)

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



NEW QUESTION 1

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

NEW QUESTION 2

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

NEW QUESTION 3

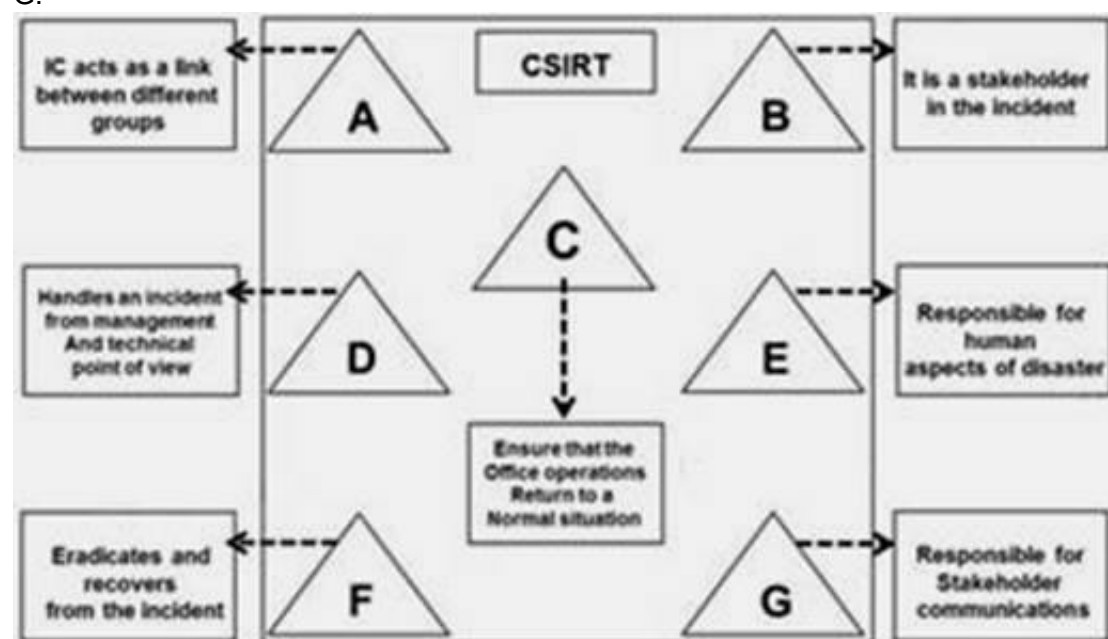
Business continuity is defined as the ability of an organization to continue to function even after a disastrous event, accomplished through the deployment of redundant hardware and software, the use of fault tolerant systems, as well as a solid backup and recovery strategy. Identify the plan which is 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 4

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 5

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 6

An incident recovery plan is a statement of actions that should be taken before, during or after an incident. Identify which of the following is NOT an objective of the incident recovery plan?

- A. Creating new business processes to maintain profitability after incident
- B. Providing a standard for testing the recovery plan
- C. Avoiding the legal liabilities arising due to incident
- D. Providing assurance that systems are reliable

Answer: A

NEW QUESTION 7

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 8

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 9

Computer forensics is methodical series of techniques and procedures for gathering evidence from computing equipment, various storage devices and or digital media that can be presented in a court of law in a coherent and meaningful format. Which one of the following is an appropriate flow of steps in the computer forensics process:

- A. Examination > Analysis > Preparation > Collection > Reporting
- B. Preparation > Analysis > Collection > Examination > Reporting
- C. Analysis > Preparation > Collection > Reporting > Examination
- D. Preparation > Collection > Examination > Analysis > Reporting

Answer: D

NEW QUESTION 10

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 10

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 12

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 13

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 16

A threat source does not present a risk if NO vulnerability that can be exercised for a particular threat source. Identify the step in which different threat sources are defined:



- A. Identification Vulnerabilities
- B. Control analysis
- C. Threat identification
- D. System characterization

Answer: C

NEW QUESTION 21

Which of the following incident recovery testing methods works by creating a mock disaster, like fire to identify the reaction of the procedures that are implemented to handle such situations?

- A. Scenario testing
- B. Facility testing
- C. Live walk-through testing
- D. Procedure testing

Answer: D

NEW QUESTION 23

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 27

One of the main objectives of incident management is to prevent incidents and attacks by tightening the physical security of the system or infrastructure. According to CERT's incident management process, which stage focuses on implementing infrastructure improvements resulting from postmortem reviews or other process improvement mechanisms?

- A. Protection
- B. Preparation
- C. Detection
- D. Triage

Answer: A

NEW QUESTION 31

Risk management consists of three processes, risk assessment, mitigation and evaluation. Risk assessment determines the extent of the potential threat and the risk associated with an IT system through its SDLC. How many primary steps does NIST's risk assessment methodology involve?

- A. Twelve
- B. Four
- C. Six
- D. Nine

Answer: D

NEW QUESTION 32

Which policy recommends controls for securing and tracking organizational resources:

- A. Access control policy
- B. Administrative security policy
- C. Acceptable use policy
- D. Asset control policy

Answer: D

NEW QUESTION 36

Organizations or incident response teams need to protect the evidence for any future legal actions that may be taken against perpetrators that intentionally attacked the computer system. EVIDENCE PROTECTION is also required to meet legal compliance issues. Which of the following documents helps in protecting evidence from physical or logical damage:

- A. Network and host log records
- B. Chain-of-Custody
- C. Forensic analysis report
- D. Chain-of-Precedence

Answer: B

NEW QUESTION 38

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 41

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 45

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 48

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 50

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 55

The type of relationship between CSIRT and its constituency have an impact on the services provided by the CSIRT. Identify the level of the authority that enables members of CSIRT to undertake any necessary actions on behalf of their constituency?

- A. Full-level authority
- B. Mid-level authority
- C. Half-level authority
- D. Shared-level authority

Answer: A

NEW QUESTION 56

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 58

A computer forensic investigator must perform a proper investigation to protect digital evidence. During the investigation, an investigator needs to process large amounts of data using a combination of automated and manual methods. Identify the computer forensic process involved:

- A. Analysis
- B. Preparation
- C. Examination
- D. Collection

Answer: C

NEW QUESTION 59

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 61

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 65

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 68

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 69

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 73

Which of the following is a risk assessment tool:

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

Answer: C

NEW QUESTION 76

Performing Vulnerability Assessment is an example of a:

- A. Incident Response
- B. Incident Handling
- C. Pre-Incident Preparation
- D. Post Incident Management

Answer: C

NEW QUESTION 77

Preventing the incident from spreading and limiting the scope of the incident is known as:

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

Answer: C

NEW QUESTION 80

What is the best staffing model for an incident response team if current employees' expertise is very low?

- A. Fully outsourced
- B. Partially outsourced
- C. Fully insourced
- D. All the above

Answer: A

NEW QUESTION 82

Which of the following is an incident tracking, reporting and handling tool:

- A. CRAMM
- B. RTIR
- C. NETSTAT
- D. EAR/ Pilar

Answer: B

NEW QUESTION 85

Incident Response Plan requires

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

Answer: D

NEW QUESTION 87

The service organization that provides 24x7 computer security incident response services to any user, company, government agency, or organization is known as:

- A. Computer Security Incident Response Team CSIRT
- B. Security Operations Center SOC
- C. Digital Forensics Examiner

D. Vulnerability Assessor

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

The role that applies appropriate technology and tries to eradicate and recover from the incident is known as:

- A. Incident Manager
- B. Incident Analyst
- C. Incident Handler
- D. Incident coordinator

Answer: B

NEW QUESTION 96

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 98

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 100

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

An active vulnerability scanner featuring high speed discovery, configuration auditing, asset profiling, sensitive data discovery, and vulnerability analysis is called:

- A. Nessus
- B. CyberCop
- C. EtherApe
- D. nmap

Answer: A

NEW QUESTION 105

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 108

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 111

The open source TCP/IP network intrusion prevention and detection system (IDS/IPS), uses a rule-driven language, performs real-time traffic analysis and packet logging is known as:

- A. Snort
- B. Wireshark
- C. Nessus
- D. SAINT

Answer: A

NEW QUESTION 112

A Malicious code attack using emails is considered as:

- A. Malware based attack
- B. Email attack
- C. Inappropriate usage incident
- D. Multiple component attack

Answer: D

NEW QUESTION 116

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 117

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 121

_____ attach(es) to files

- A. adware
- B. Spyware
- C. Viruses
- D. Worms

Answer: C

NEW QUESTION 124

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 125

The Malicious code that is installed on the computer without user's knowledge to acquire information from the user's machine and send it to the attacker who can access it remotely is called:

- A. Spyware
- B. Logic Bomb
- C. Trojan
- D. Worm

Answer: A

NEW QUESTION 127

Which of the following is NOT one of the common techniques used to detect Insider threats:

- A. Spotting an increase in their performance
- B. Observing employee tardiness and unexplained absenteeism
- C. Observing employee sick leaves
- D. Spotting conflicts with supervisors and coworkers

Answer: A

NEW QUESTION 132

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 136

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 139

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 144

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 146

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 151

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 153

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 158

To recover, analyze, and preserve computer and related materials in such a way that it can be presented as evidence in a court of law and identify the evidence in short time, estimate the potential impact of the malicious activity on the victim, and assess the intent and identity of the perpetrator is known as:

- A. Computer Forensics
- B. Digital Forensic Analysis
- C. Forensic Readiness
- D. Digital Forensic Examiner

Answer: B

NEW QUESTION 161

Any information of probative value that is either stored or transmitted in a digital form during a computer crime is called:

- A. Digital evidence
- B. Computer Emails
- C. Digital investigation
- D. Digital Forensic Examiner

Answer: A

NEW QUESTION 164

Which of the following is NOT one of the Computer Forensic types:

- A. USB Forensics
- B. Email Forensics
- C. Forensic Archaeology
- D. Image Forensics

Answer: C

NEW QUESTION 167

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 170

Electronic evidence may reside in the following:

- A. Data Files
- B. Backup tapes
- C. Other media sources
- D. All the above

Answer: D

NEW QUESTION 174

A methodical series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media, that can be presented in a court of law in a coherent and meaningful format is called:

- A. Forensic Analysis
- B. Computer Forensics
- C. Forensic Readiness
- D. Steganalysis

Answer: B

NEW QUESTION 179

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 183

Incident may be reported using/ by:

- A. Phone call
- B. Facsimile (Fax)
- C. Email or on-line Web form
- D. All the above

Answer: D

NEW QUESTION 186

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 190

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 195

The steps followed to recover computer systems after an incident are:

- A. System restoration, validation, operation and monitoring
- B. System restoration, operation, validation, and monitoring
- C. System monitoring, validation, operation and restoration
- D. System validation, restoration, operation and monitoring

Answer: A

NEW QUESTION 199

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 201

.....

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