

EC-Council

Exam Questions 212-89

EC Council Certified Incident Handler (ECIH v2)



NEW QUESTION 1

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

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

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

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 5

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 course 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 6

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 7

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 8

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 9

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 10

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 10

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 12

Computer viruses are malicious software programs that infect computers and corrupt or delete the data on them. Identify the virus type that specifically infects Microsoft Word files?

- A. Micro Virus
- B. File Infector
- C. Macro Virus
- D. Boot Sector virus

Answer: C

NEW QUESTION 15

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 17

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. Introductory approach
- C. Proactive approach
- D. Qualitative approach

Answer: C

NEW QUESTION 22

The largest number of cyber-attacks are conducted by:

- A. Insiders
- B. Outsiders
- C. Business partners
- D. Suppliers

Answer: B

NEW QUESTION 26

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

The left over risk after implementing a control is called:

- A. Residual risk
- B. Unaccepted risk
- C. Low risk
- D. Critical risk

Answer: A

NEW QUESTION 36

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 39

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 44

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 49

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 53

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 54

Common name(s) for CSIRT is(are)

- A. Incident Handling Team (IHT)
- B. Incident Response Team (IRT)
- C. Security Incident Response Team (SIRT)
- D. All the above

Answer: D

NEW QUESTION 55

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 60

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 62

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 64

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 67

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 69

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 70

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 73

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 75

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 80

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 84

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 87

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 92

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 94

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 95

Bit stream image copy of the digital evidence must be performed in order to:

- A. Prevent alteration to the original disk
- B. Copy the FAT table
- C. Copy all disk sectors including slack space
- D. All the above

Answer: C

NEW QUESTION 98

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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 First Try
- * 212-89 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 212-89 Practice Test Here](#)