

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

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 4

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 5

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 6

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 7

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 8

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 9

Which one of the following is the correct sequence of flow of the stages in an incident response:

- A. Containment - Identification - Preparation - Recovery - Follow-up - Eradication
- B. Preparation - Identification - Containment - Eradication - Recovery - Follow-up
- C. Eradication - Containment - Identification - Preparation - Recovery - Follow-up
- D. Identification - Preparation - Containment - Recovery - Follow-up - Eradication

Answer: B

NEW QUESTION 10

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 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 11

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 13

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 17

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 19

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 24

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 28

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 33

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 35

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 36

Incident Response Plan requires

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

Answer: D

NEW QUESTION 40

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 44

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 47

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 50

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 54

_____ attach(es) to files

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

Answer: C

NEW QUESTION 55

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 59

Which is the incorrect statement about Anti-keyloggers scanners:

- A. Detect already installed Keyloggers in victim machines
- B. Run in stealthy mode to record victims online activity
- C. Software tools

Answer: B

NEW QUESTION 64

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 69

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 74

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 78

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 83

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 87

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 88

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 89

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

Answer: D

NEW QUESTION 93

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 98

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 100

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 101

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 103

.....

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](#)