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

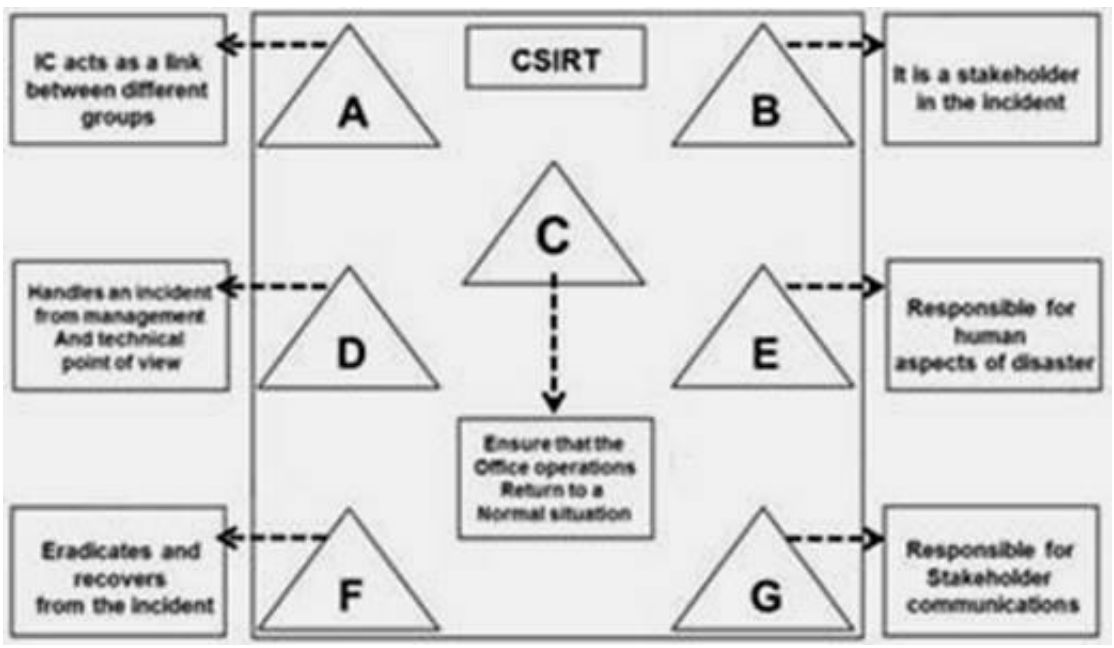
Answer: A

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
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 6
Identify the network security incident where intended authorized users are prevented from using system, network, or applications by flooding the network with high volume of traffic that consumes all existing network
resources.

A. URL Manipulation
B. XSS Attack
C. SQL Injection
D. Denial of Service Attack

Answer: D

NEW QUESTION 7
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 8
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 9
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 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 11
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 13
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 17
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 19
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 22
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 23
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 28
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 31
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 32
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 33
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 36
The IDS and IPS system logs indicating an unusual deviation from typical network traffic flows; this is called:

A. A Precursor
B. An Indication
C. A Proactive
D. A Reactive

Answer: B

NEW QUESTION 40
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 41
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 42
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 44
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 46
Which of the following is a risk assessment tool:

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

Answer: C

NEW QUESTION 50
The correct sequence of Incident Response and Handling is:

A. Incident Identification, recording, initial response, communication and containment
B. Incident Identification, initial response, communication, recording and containment
C. Incident Identification, communication, recording, initial response and containment
D. Incident Identification, recording, initial response, containment and communication

Answer: A

NEW QUESTION 51
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 53
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 58
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 62
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 63
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 67
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 68
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 72
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 76
Changing the web server contents, Accessing the workstation using a false ID and Copying sensitive data without authorization are examples of:

A. DDoS attacks
B. Unauthorized access attacks
C. Malware attacks
D. Social Engineering attacks

Answer: B

NEW QUESTION 78
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 81
In a DDoS attack, attackers first infect multiple systems, which are then used to attack a particular target directly. Those systems are called:

A. Honey Pots
B. Relays
C. Zombies
D. Handlers

Answer: C

NEW QUESTION 85
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 89
_____ attach(es) to files

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

Answer: C

NEW QUESTION 92
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 93
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 94
A Host is infected by worms that propagates through a vulnerable service; the sign(s) of the presence of the worm include:

A. Decrease in network usage
B. Established connection attempts targeted at the vulnerable services
C. System becomes instable or crashes
D. All the above

Answer: C

NEW QUESTION 99
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 101
Keyloggers do NOT:

A. Run in the background
B. Alter system files
C. Secretly records URLs visited in browser, keystrokes, chat conversations, ...etc
D. Send log file to attacker's email or upload it to an ftp server

Answer: B

NEW QUESTION 102
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 105
Insiders may be:

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

Answer: D

NEW QUESTION 106
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 107
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 110
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 115
The correct order or sequence of the Computer Forensic processes is:

A. Preparation, analysis, examination, collection, and reporting
B. Preparation, collection, examination, analysis, and reporting
C. Preparation, examination, collection, analysis, and reporting
D. Preparation, analysis, collection, examination, and reporting

Answer: B

NEW QUESTION 117
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 118
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 120
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 125
Which test is conducted to determine the incident recovery procedures effectiveness?

A. Live walk-throughs of procedures
B. Scenario testing
C. Department-level test
D. Facility-level test

Answer: A

NEW QUESTION 128
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 131
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 policyAn information security policy must be:
E. Distributed and communicated
F. Enforceable and Regularly updated
G. Written in simple language
H. All the above

Answer: D

NEW QUESTION 136
The most common type(s) of intellectual property is(are):

A. Copyrights and Trademarks
B. Patents
C. Industrial design rights & Trade secrets
D. All the above

Answer: D

NEW QUESTION 137
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 139
.....

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