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.

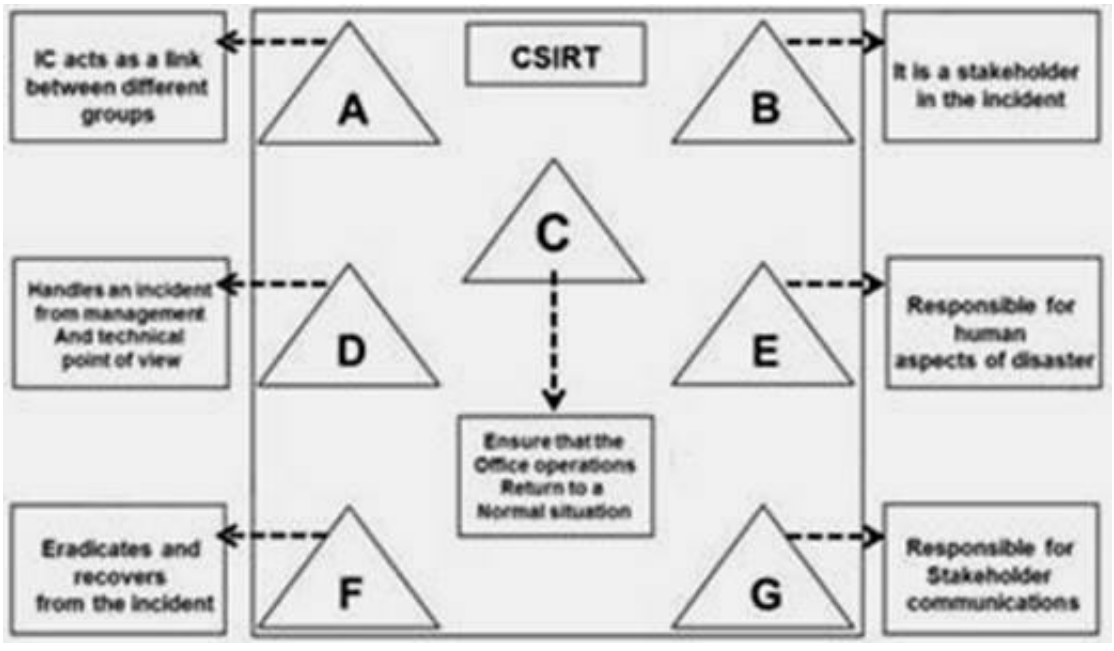
Answer: A

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
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
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 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
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
A US Federal agency network was the target of a DoS attack that prevented and impaired the normal authorized functionality of the networks. According to agency's reporting timeframe guidelines, this incident
should be reported within two (2) HOURS of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate the activity. Which incident category of the US Federal Agency does this incident belong to?

A. CAT 5
B. CAT 1
C. CAT 2
D. CAT 6

Answer: C

NEW QUESTION 10
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 10
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 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 15
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 21
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 22
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 23
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 28
The insider risk matrix consists of technical literacy and business process knowledge vectors. Considering the matrix, one can conclude that:

A. If the insider's technical literacy is low and process knowledge is high, the risk posed by the threat will be insignificant.
B. If the insider's technical literacy and process knowledge are high, the risk posed by the threat will be insignificant.
C. If the insider's technical literacy is high and process knowledge is low, the risk posed by the threat will be high.
D. If the insider's technical literacy and process knowledge are high, the risk posed by the threat will be high.

Answer: D

NEW QUESTION 30
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 34
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 39
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 42
A security policy will take the form of a document or a collection of documents, depending on the situation or usage. It can become a point of reference in case a violation occurs that results in dismissal or other penalty. Which of the following is NOT true for a good security policy?

A. It must be enforceable with security tools where appropriate and with sanctions where actual prevention is not technically feasible
B. It must be approved by court of law after verifications of the stated terms and facts
C. It must be implemented through system administration procedures, publishing of acceptable use guide lines or other appropriate methods
D. It must clearly define the areas of responsibilities of the users, administrators and management

Answer: B

NEW QUESTION 46
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 50
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 53
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 57
A risk mitigation strategy determines the circumstances under which an action has to be taken to minimize and overcome risks. Identify the risk mitigation strategy that focuses on minimizing the probability of risk and losses by searching for vulnerabilities in the system and appropriate controls:

A. Risk Assumption
B. Research and acknowledgment
C. Risk limitation
D. Risk absorption

Answer: B

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 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 65
The largest number of cyber-attacks are conducted by:

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

Answer: B

NEW QUESTION 70
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 72
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
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 74
Which of the following is a risk assessment tool:

A. Nessus

B. Wireshark
C. CRAMM
D. Nmap

Answer: C

NEW QUESTION 79
In NIST risk assessment/ methodology; the process of identifying the boundaries of an IT system along with the resources and information that constitute the system is known as:

A. Asset Identification
B. System characterization
C. Asset valuation
D. System classification

Answer: B

NEW QUESTION 83
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 85
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 90
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 93
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 94
Which of the following service(s) is provided by the CSIRT:

A. Vulnerability handling
B. Technology watch
C. Development of security tools
D. All the above

Answer: D

NEW QUESTION 95
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 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 100
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 103
The typical correct sequence of activities used by CSIRT when handling a case is:

A. Log, inform, maintain contacts, release information, follow up and reporting
B. Log, inform, release information, maintain contacts, follow up and reporting
C. Log, maintain contacts, inform, release information, follow up and reporting
D. Log, maintain contacts, release information, inform, follow up and reporting

Answer: A

NEW QUESTION 107
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 110
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 112
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 115

A malicious security-breaking code that is disguised as any useful program that installs an executable programs when a file is opened and allows others to control the victim's system is called:

A. Trojan
B. Worm
C. Virus
D. RootKit

Answer: A

NEW QUESTION 118
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 119
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 120
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 121
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 125
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 129
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 131
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 136
Spyware tool used to record malicious user's computer activities and keyboard stokes is called:

A. adware
B. Keylogger
C. Rootkit
D. Firewall

Answer: B

NEW QUESTION 141
Insiders may be:

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

Answer: D

NEW QUESTION 144
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 149
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 152
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 154
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 159
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 160
Digital evidence must:

A. Be Authentic, complete and reliable
B. Not prove the attackers actions
C. Be Volatile
D. Cast doubt on the authenticity and veracity of the evidence

Answer: A

NEW QUESTION 162
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 172
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 177
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 181
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 185
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 188
.....

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