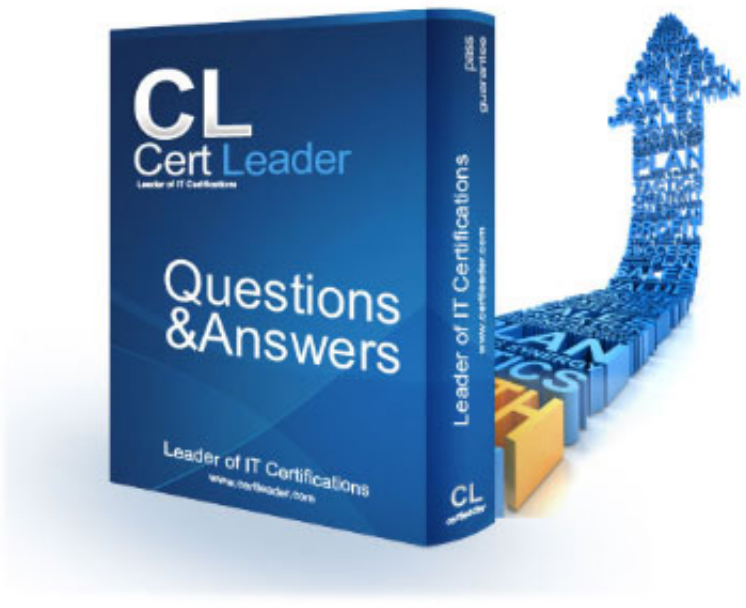
212-89 Dumps

EC Council Certified Incident Handler (ECIH v2)

https://www.certleader.com/212-89-dumps.html



NEW QUESTION 1
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

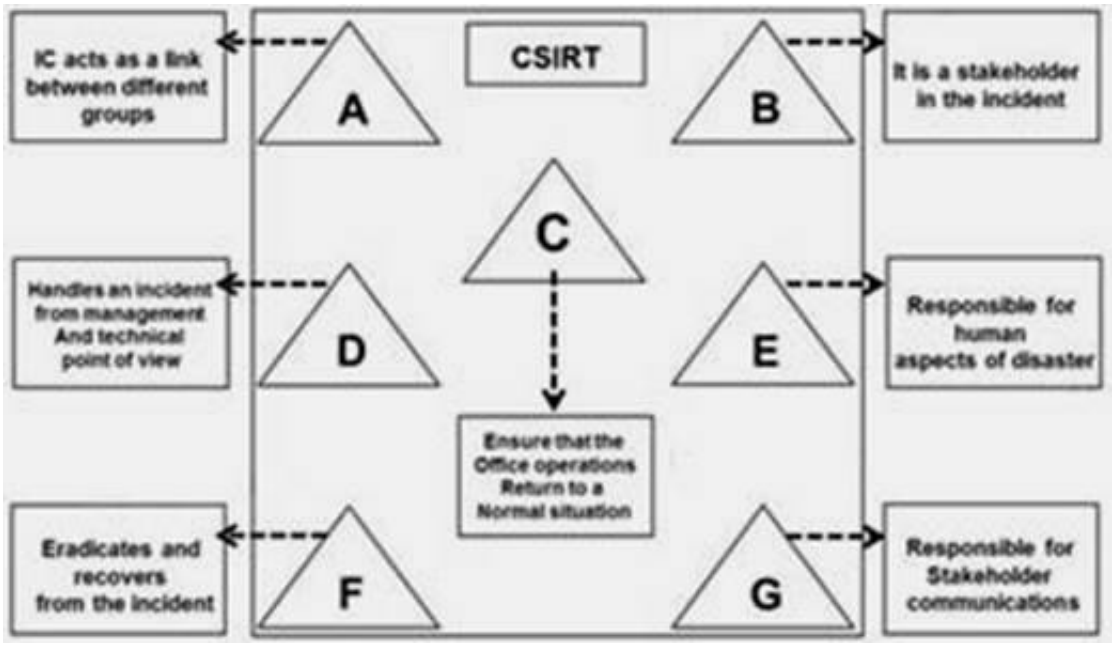
Answer: A

NEW QUESTION 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
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
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 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
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 7
Quantitative risk is the numerical determination of the probability of an adverse event and the extent of the losses due to the event. Quantitative risk is calculated as:

A. (Probability of Loss) X (Loss)
B. (Loss) / (Probability of Loss)
C. (Probability of Loss) / (Loss)
D. Significant Risks X Probability of Loss X Loss

Answer: A

NEW QUESTION 8
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 9
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 10
Identify a standard national process which establishes a set of activities, general tasks and a management structure to certify and accredit systems that will maintain the information assurance (IA) and security posture of a system or site.

A. NIASAP
B. NIAAAP
C. NIPACP
D. NIACAP

Answer: D

NEW QUESTION 12
Policies are designed to protect the organizational resources on the network by establishing the set rules and procedures. Which of the following policies authorizes a group of users to perform a set of actions on a set of resources?

A. Access control policy
B. Audit trail policy
C. Logging policy
D. Documentation policy

Answer:

A

NEW QUESTION 15
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 19
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 24
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 28
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
Insider threats can be detected by observing concerning behaviors exhibited by insiders, such as conflicts with supervisors and coworkers, decline in performance, tardiness or unexplained absenteeism. Select the technique that helps in detecting insider threats:

A. Correlating known patterns of suspicious and malicious behavior
B. Protecting computer systems by implementing proper controls
C. Making is compulsory for employees to sign a none disclosure agreement
D. Categorizing information according to its sensitivity and access rights

Answer: A

NEW QUESTION 37
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 41

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 42
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 43
A computer virus hoax is a message warning the recipient of non-existent computer virus. The message is usually a chain e-mail that tells the recipient to forward it to every one they know. Which of the following is NOT a symptom of virus hoax message?

A. The message prompts the end user to forward it to his / her e-mail contact list and gain monetary benefits in doing so
B. The message from a known email id is caught by SPAM filters due to change of filter settings
C. The message warns to delete certain files if the user does not take appropriate action
D. The message prompts the user to install Anti-Virus

Answer: A

NEW QUESTION 46
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 48
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 53
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 58
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 60
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 64
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. Introductive approach
C. Proactive approach
D. Qualitative approach

Answer: C

NEW QUESTION 66
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 69
The sign of incident that may happen in the future is called:

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

Answer: A

NEW QUESTION 70
An information security incident is

A. Any real or suspected adverse event in relation to the security of computer systems or networks
B. Any event that disrupts normal today's business functions
C. Any event that breaches the availability of information assets
D. All of the above

Answer: D

NEW QUESTION 72
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 74
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 78
Absorbing minor risks while preparing to respond to major ones is called:

A. Risk Mitigation
B. Risk Transfer
C. Risk Assumption
D. Risk Avoidance

Answer: C

NEW QUESTION 80
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 85
What is correct about Quantitative Risk Analysis:

A. It is Subjective but faster than Qualitative Risk Analysis
B. Easily automated
C. Better than Qualitative Risk Analysis
D. Uses levels and descriptive expressions

Answer: B

NEW QUESTION 90
Which of the following is a risk assessment tool:

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

Answer: C

NEW QUESTION 95
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 100
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 103
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 106
Removing or eliminating the root cause of the incident is called:

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

Answer: A

NEW QUESTION 109
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 112
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 116
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 117
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 119
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 121
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 123
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 126
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 129
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 131
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 132
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 136
Which of the following is a characteristic of adware?

A. Gathering information
B. Displaying popups
C. Intimidating users
D. Replicating

Answer: B

NEW QUESTION 141
_____ attach(es) to files

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

Answer: C

NEW QUESTION 146
The free utility which quickly scans Systems running Windows OS to find settings that may have been changed by spyware, malware, or other unwanted programs is called:

A. Tripwire
B. HijackThis
C. Stinger
D. F-Secure Anti-virus

Answer: B

NEW QUESTION 147
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 150
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 151
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 153
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 156
Insiders may be:

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

Answer: D

NEW QUESTION 161
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 163
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 168
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 173
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 176
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 180
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 182
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 187
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 190
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 193
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 196
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 200
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 204
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 212-89 Exam with Our Prep Materials Via below:

https://www.certleader.com/212-89-dumps.html