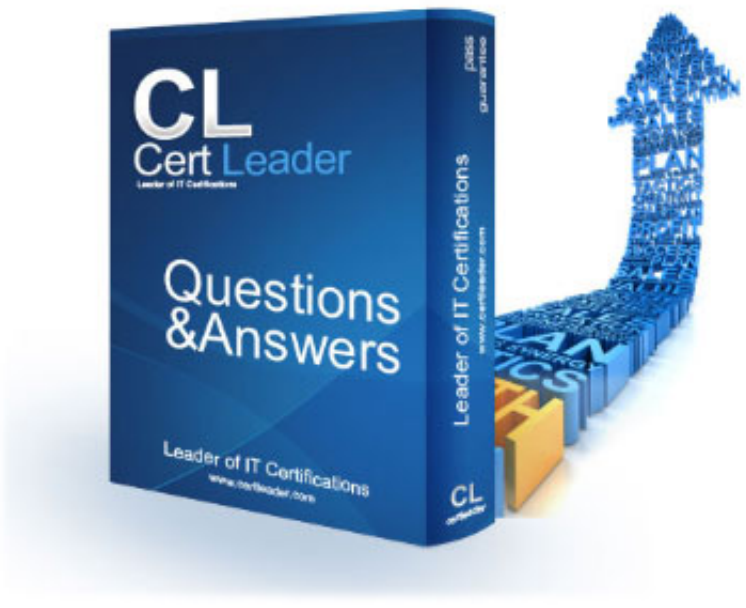
212-89 Dumps

EC Council Certified Incident Handler (ECIH v2)

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



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
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 3
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 4
Risk is defined as the probability of the occurrence of an incident. Risk formulation generally begins with the likeliness of an event’s occurrence, the harm it may cause and is usually denoted as Risk = ?(events)X (Probability of occurrence)X?

A. Magnitude
B. Probability
C. Consequences
D. Significance

Answer: A

NEW QUESTION 5
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 6
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 7
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 8
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 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
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 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 11
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 15
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 19
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 23
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 26
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 30
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 33
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 34
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 36
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 39
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 40
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 44
The largest number of cyber-attacks are conducted by:

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

Answer: B

NEW QUESTION 49
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 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 52
Incident response team must adhere to the following:

A. Stay calm and document everything
B. Assess the situation
C. Notify appropriate personnel
D. All the above

Answer: D

NEW QUESTION 57
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 59
Incident Response Plan requires

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

Answer: D

NEW QUESTION 64
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 65
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 67
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 72
Installing a password cracking tool, downloading pornography material, sending emails to colleagues which irritates them and hosting unauthorized websites on the company's computer are considered:

A. Network based attacks
B. Unauthorized access attacks
C. Malware attacks
D. Inappropriate usage incidents

Answer: D

NEW QUESTION 75
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 78
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 80
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 81
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 85
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 87
The sign(s) of the presence of malicious code on a host infected by a virus which is delivered via e-mail could be:

A. Antivirus software detects the infected files
B. Increase in the number of e-mails sent and received
C. System files become inaccessible
D. All the above

Answer: D

NEW QUESTION 90
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 95
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 97
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 102
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 107
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 109
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 114
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
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 120
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 121
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 123
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 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 127
Business Continuity provides a planning methodology that allows continuity in business operations:

A. Before and after a disaster
B. Before a disaster
C. Before, during and after a disaster
D. During and after a disaster

Answer: C

NEW QUESTION 132
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 137
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 142
According to the Evidence Preservation policy, a forensic investigator should make at least ..... image copies of the digital evidence.

A. One image copy
B. Two image copies
C. Three image copies
D. Four image copies

Answer: B

NEW QUESTION 146
.....

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