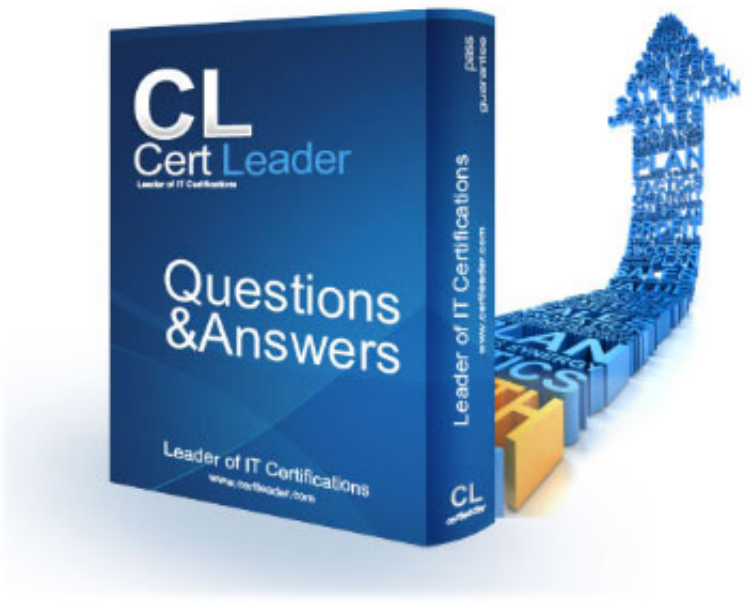
212-89 Dumps

EC Council Certified Incident Handler (ECIH v2)

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



NEW QUESTION 1
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 2
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 3
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 4
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 5
US-CERT and Federal civilian agencies use the reporting timeframe criteria in the federal agency reporting categorization. What is the timeframe required to report an incident under the CAT 4 Federal Agency category?

A. Weekly
B. Within four (4) hours of discovery/detection if the successful attack is still ongoing and agency is unable to successfully mitigate activity
C. Within two (2) hours of discovery/detection
D. Monthly

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
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 8
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 9
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 10
In a qualitative risk analysis, risk is calculated in terms of:

A. (Attack Success + Criticality) –(Countermeasures)
B. Asset criticality assessment – (Risks and Associated Risk Levels)
C. Probability of Loss X Loss
D. (Countermeasures + Magnitude of Impact) – (Reports from prior risk assessments)

Answer: C

NEW QUESTION 10
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 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. Introductive approach
C. Proactive approach
D. Qualitative approach

Answer: C

NEW QUESTION 17
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 20
Total cost of disruption of an incident is the sum of

A. Tangible and Intangible costs
B. Tangible cost only

C. Intangible cost only
D. Level Two and Level Three incidents cost

Answer: A

NEW QUESTION 23
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 26
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 29
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 31
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 33
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 37
_____ attach(es) to files

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

Answer: C

NEW QUESTION 38
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 40
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 42
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 43
Which of the following is NOT one of the techniques used to respond to insider threats:

A. Placing malicious users in quarantine network, so that attack cannot be spread
B. Preventing malicious users from accessing unclassified information
C. Disabling the computer systems from network connection
D. Blocking malicious user accounts

Answer: B

NEW QUESTION 47
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 48
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 52
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 53
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 58
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 62
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 67
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 70
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 71
.....

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