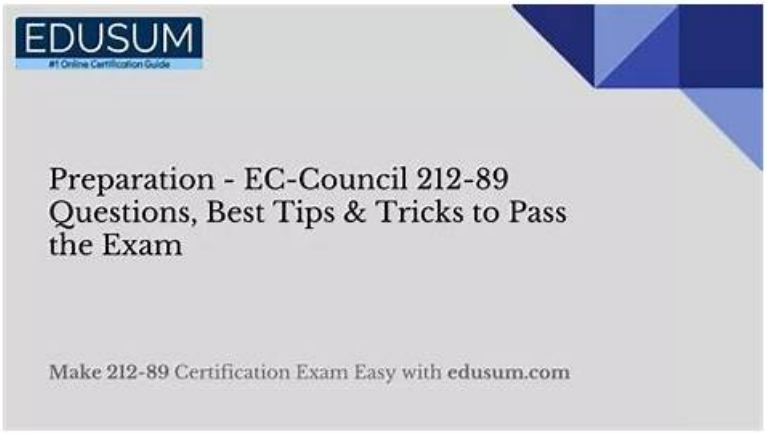
212-89 Valuable Feedback & 212-89 Unlimited Exam Practice



P.S. Free & New 212-89 dumps are available on Google Drive shared by PassLeaderVCE: https://drive.google.com/open?id=1Lp8IXT7BHQeQsn3jRjTS3eqoVfulFWOP

Many customers may doubt the quality of our EC-COUNCIL 212-89 learning quiz since they haven't tried them. But our 212-89 training engine is reliable. What you have learnt on our EC Council Certified Incident Handler (ECIH v3) 212-89 Exam Materials are going through special selection. The core knowledge of the real exam is significant.

EC-COUNCIL ECIH certification is an ideal program for entry-level cybersecurity professionals, network administrators, security architects, and engineers. It is also recommended for IT professionals looking to advance their careers in security management, governance, and risk mitigation. EC Council Certified Incident Handler (ECIH v3) certification builds a strong base for individuals to enter into more advanced security certifications such as EC-Council Certified Ethical Hacker, Certified Network Defender or Certified Hacking Forensic Investigator.

The EC Council Certified Incident Handler (ECIH v2) certification is a highly specialized credential designed for professionals who are involved in incident handling, response, and analysis. The ECIH v2 certification exam is designed to test the knowledge, skills, and abilities of candidates in the areas of incident handling and response, computer forensics, and network security. EC Council Certified Incident Handler (ECIH v3) certification is recognized globally and is highly valued by employers and IT security professionals.

>> 212-89 Valuable Feedback <<

EC-COUNCIL 212-89 Unlimited Exam Practice - Free 212-89 Exam

Our 212-89 question materials are designed to help ambitious people. The nature of human being is pursuing wealth and happiness. Perhaps you still cannot make specific decisions. It doesn't matter. We have the free trials of the 212-89 study materials for you. The initiative is in your own hands. Our 212-89 Exam Questions are very outstanding. People who have bought our products praise our company highly. In addition, we have strong research competence. So you can always study the newest version of the 212-89 exam questions.

The ECIH v2 certification is ideal for IT professionals who are responsible for incident handling, including security analysts, network administrators, security engineers, and incident responders. EC Council Certified Incident Handler (ECIH v3) certification is also suitable for IT managers who oversee incident response teams and need to understand the incident handling process. EC Council Certified Incident Handler (ECIH v3) certification is globally recognized and provides a valuable credential for IT professionals who want to advance their careers in the cybersecurity industry.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q47-Q52):

NEW QUESTION # 47
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. Facility testing
- B. Scenario testing
- C. Live walk-through testing
- D. Procedure testing

Answer: D

NEW QUESTION # 48
Which of the following is not the responsibility of first responders?

- A. Packaging and transporting the electronic evidence
- B. Preserving temporary and fragile evidence and then shut down or reboot the victim's computer
- C. Protecting the crime scene
- D. Identifying the crime scene

Answer: B

Explanation:
The responsibility of first responders does not include shutting down or rebooting the victim's computer as a measure to preserve temporary and fragile evidence. In fact, such actions can potentially alter or destroy volatile data that could be crucial for the investigation. The primary responsibilities of first responders include protecting and identifying the crime scene, and ensuring the preservation of evidence in its original state as much as possible, which may involve isolating affected systems from the network but not necessarily shutting them down or rebooting them without proper forensic readiness and consideration.

NEW QUESTION # 49
An attacker after performing an attack decided to wipe evidences using artifact wiping techniques to evade forensic investigation. He applied magnetic field to the digital media device, resulting in an entirely clean device of any previously stored data.
Identify the artifact wiping technique used by the attacker.

- A. Disk cleaning utilities
- B. File wiping utilities
- C. Disk degaussing/destruction
- D. Syscall proxying

Answer: C

Explanation:
The technique described, where an attacker applies a magnetic field to a digital media device to clean it of any previously stored data, is known as disk degaussing. Degaussing is a method used to erase a disk or tape by exposing it to a strong magnetic field, destroying the magnetic data storage mechanism and leaving the device clean of any data. This process is effectively used for wiping digital evidence in a way that makes recovery impossible, serving as a method of anti-forensics. Unlike file wiping utilities or disk cleaning utilities, which overwrite or delete data (potentially leaving traces that can be recovered), degaussing physically alters the storage medium itself, making data recovery unfeasible.
References:The ECIH v3 certification program discusses various artifact wiping techniques, including degaussing, as part of understanding anti-forensic methods that attackers use to evade detection and investigation.

NEW QUESTION # 50
A cybersecurity team at a financial services firm detects abnormal behavior on several endpoints, suggesting a possible breach. The anomalies include unexpected data transfers and processes running with unusual permissions. Given the potential impact, the team needs to quickly validate whether these are indicators of a security incident or benign anomalies. What method should the team prioritize to detect and validate the incident effectively?

- A. Engage an external cybersecurity consultancy to conduct an independent assessment.
- B. Disconnect the affected endpoints from the network to prevent potential data exfiltration.
- C. Implement strict access control measures to limit permissions on all endpoints immediately.
- D. Utilize an advanced behavioral analysis tool to differentiate between legitimate and malicious activities.

Answer: D

Explanation:
Explanation (aligned to IH&R lifecycle):
This question is about triage/validation-determining whether what you see is truly an incident and establishing priority. The most appropriate first move is to use endpoint telemetry and behavioral analytics (A) to validate maliciousness (e.g., suspicious parent/child process chains, token manipulation, credential dumping patterns, anomalous privilege escalation, and data transfer behaviors). This supports fast, evidence- based classification and reduces unnecessary disruption. Option (C) is containment and may be required after validation or for clearly high-confidence cases, but immediately disconnecting multiple endpoints can destroy volatile evidence, break business operations, and reduce your ability to trace lateral movement patterns across hosts. Option (B) is a broad preventive change that can create outage risk and is not a validation method.
Option (D) can be helpful, but it is slower and not the primary "detect and validate" action for an internal team facing active anomalies.
A disciplined approach is: validate via behavioral tooling + logs, scope affected endpoints, determine severity, then execute containment proportional to confirmed risk. That sequencing mirrors standard incident handling flow (identify # validate/triage # contain # eradicate # recover # lessons learned). When time matters, the highest-value action is the one that converts ambiguous signals into confident incident classification quickly- behavioral validation does that best.

NEW QUESTION # 51
Dan is a newly appointed information security professional in a renowned organization. He is supposed to follow multiple security strategies to eradicate malware incidents. Which of the following is not considered as a good practice for maintaining information security and eradicating malware incidents?

- A. Do not open files with file extensions such as .bat, .com, ,exe, .pif, .vbs, and so on
- B. Do not click on web browser pop-up windows
- C. Do not download or execute applications from third-party sources
- D. Do not download or execute applications from trusted sources

Answer: D

NEW QUESTION # 52
.....

- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, active-bookmarks.com, www.stes.tyc.edu.tw, estar.jp, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.citylifenews.net, www.ted.com, Disposable vapes

P.S. Free & New 212-89 dumps are available on Google Drive shared by PassLeaderVCE: https://drive.google.com/open?id=1Lp8IXT7BHQeQsn3jRjTS3eqoVfuIFWOP