Latest 212-89 Exam Vce & Reliable Study 212-89 Questions

P.S. Free 2026 EC-COUNCIL 212-89 dumps are available on Google Drive shared by Prep4sureGuide: https://drive.google.com/open?id=1B2pNv_ECEDxlH485Nq4ftLUbQAPIsZX4

Prep4sureGuide online digital EC-COUNCIL 212-89 exam questions are the best way to prepare. Using our EC-COUNCIL 212-89 exam dumps, you will not have to worry about whatever topics you need to master. To practice for a EC-COUNCIL 212-89 Certification Exam in the Prep4sureGuide (free test), you should perform a self-assessment. The 212-89 practice test Prep4sureGuide keeps track of each previous attempt and highlights the improvements with each attempt.

There are topics of ECCouncil 212-89 Exam

Candidates must know the exam topics before they start of preparation. Because it will really help them in hitting the core. Our **ECCouncil 212-89 exam dumps** will include the following topics:

- Forensic Readiness and First Response
- Handling and Responding to Email Security Incidents
- Introduction to Incident Handling and Response
- Handling and Responding to Cloud Security Incidents

>> Latest 212-89 Exam Vce <<

Latest 212-89 Exam Vce - EC-COUNCIL Realistic Latest EC Council Certified Incident Handler (ECIH v3) Exam Vce Pass Guaranteed Quiz

The EC Council Certified Incident Handler (ECIH v3) (212-89) practice tests have customizable time and EC Council Certified Incident Handler (ECIH v3) (212-89) exam questions feature so that the students can set the time and EC Council Certified Incident Handler (ECIH v3) (212-89) exam questions according to their needs. The EC Council Certified Incident Handler (ECIH v3) (212-89) practice test questions are getting updated on the daily basis and there are also up to 1 year of free updates. Earning the EC Council Certified Incident Handler (ECIH v3) (212-89) certification exam is the way to grow in the modern era with high-paying jobs.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q146-Q151):

NEW QUESTION # 146
Alex is an incident handler for Tech-o-Tech Inc. and is tasked to identify any possible insider threats within his organization. Which of the following insider threat detection techniques can be used by Alex to detect insider threats based on the behavior of a suspicious employee, both individually and in a group?

- A. Mole detection

- B. Physical detection
- C. behaviorial analysis
- D. Profiling

Answer: D

Explanation:
Behavioral analysis is a technique used to detect insider threats by analyzing the behavior of employees, both individually and in group settings, to identify any actions that deviate from the norm. This method relies on monitoring and analyzing data related to user activities, access patterns, and other behaviors that could indicate malicious intent or a potential security risk from within the organization. Behavioral analysis can detect unusual access to sensitive data, abnormal data transfer activities, and other indicators of insider threats. This approach is proactive and can help in identifying potential insider threats before they result in significant harm to the organization.
References:The Incident Handler (ECIH v3) certification materials cover various insider threat detection techniques, including the importance of behavioral analysis as a key method for identifying potential security risks posed by insiders.

NEW QUESTION # 147
Adam is an attacker who along with his team launched multiple attacks on target organization for financial benefits. Worried about getting caught, he decided to forge his identity. To do so, he created a new identity by obtaining information from different victims. Identify the type of identity theft Adam has performed.

- A. Social identity theft
- B. Medical identity theft
- C. Synthetic identity theft
- D. Tax identity theft

Answer: C

NEW QUESTION # 148
Ikeo Corp, hired an incident response team to assess the enterprise security. As part of the incident handling and response process, the IR team is reviewing the current security policies implemented by the enterprise. The IR team finds that employees of the organization do not have any restrictions on Internet access: they are allowed to visit any site, download any application, and access a computer or network from a remote location. Considering this as the main security threat, the IR team plans to change this policy as it can be easily exploited by attackers. Which of the following security policies is the IR team planning to modify?

- A. Permissive policy
- B. Promiscuous policy
- C. Prudent policy
- D. Paranoic policy

Answer: A

NEW QUESTION # 149
XYZ Inc. was affected by a malware attack and James, being the incident handling and response (IH&R) team personnel handling the incident, found out that the root cause of the incident is a backdoor that has bypassed the security perimeter due to an existing vulnerability in the deployed firewall. James had contained the spread of the infection and removed the malware completely. Now the organization asked him to perform incident impact assessment to identify the impact of the incident over the organization and he was also asked to prepare a detailed report of the incident.
Which of the following stages in IH&R process is James working on?

- A. Notification
- B. Eradication
- C. Post-incident activities
- D. Evidence gathering and forensics analysis

Answer: C

NEW QUESTION # 150
Your manager hands you several items of digital evidence and asks you to investigate them in the order of volatility. Which of the following is the MOST volatile?

- A. Temp files
- B. Disk
- C. Emails
- D. Cache

Answer: D

Explanation:
In the context of digital evidence investigation, volatility refers to how quickly data can change or be lost when power is removed or systems are altered. Among the options provided, cache is the most volatile because it is temporary storage that is designed to speed up access to data and is frequently overwritten. Cache data resides in RAM and includes things like memory buffers, system and network information, and process execution data, which are lost upon reboot or power loss. This contrasts with disks, emails, and temp files, which are considered less volatile because they are stored on permanent or semi-permanent media and are less likely to be immediately lost or overwritten.References:The Incident Handler (ECIH v3) curriculum includes principles of digital evidence handling, which emphasizes the importance of collecting evidence in descending order of volatility to ensure that the most ephemeral data is preserved before it's lost.

NEW QUESTION # 151
.....

212-89 practice test can be your optimum selection and useful tool to deal with the urgent challenge. With over a decade's striving, our 212-89 training materials have become the most widely-lauded and much-anticipated products in industry. We have three versions of 212-89 Exam Questions by modernizing innovation mechanisms and fostering a strong pool of professionals. Therefore, rest assured of full technical support from our professional elites in planning and designing 212-89 practice test.

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.stes.tyc.edu.tw, backloggd.com, Disposable vapes

2026 Latest Prep4sureGuide 212-89 PDF Dumps and 212-89 Exam Engine Free Share: https://drive.google.com/open?id=1B2pNv_ECEDxlH485Nq4ftLUbQAPIsZX4