Test 212-89 Testking & 212-89 Best Vce

P.S. Free & New 212-89 dumps are available on Google Drive shared by TestSimulate: https://drive.google.com/open?id=1_P3h-gqukh-biORajVuYkDaJ9m3OHUVy

Our evaluation system for 212-89 test material is smart and very powerful. First of all, our researchers have made great efforts to ensure that the data scoring system of our 212-89 test questions can stand the test of practicality. Once you have completed your study tasks and submitted your training results, the evaluation system will begin to quickly and accurately perform statistical assessments of your marks on the 212-89 Exam Torrent. You only need to spend 20 to 30 hours on practicing and consolidating of our 212-89 learning material, you will have a good result. After years of development practice, our 212-89 test torrent is absolutely the best. You will embrace a better future if you choose our 212-89 exam materials.

The EC-Council Certified Incident Handler (ECIH) 212-89 is an exam that prepares you for handling incidents in various information systems. It prepares you for security plans and policies to deal with incidents with efficiency & effectiveness in a time-constrained environment to decrease the effect of those incidents. This test leads you to the ECIH certification that will allow you to work as an Incident Handler and work in incident response frameworks. So, if you want to excel in the information security environment, the EC-Council Certified Incident Handler certification exam is a must for you. It will be the best gateway to a high-paying job and a good working environment, where you can work with other EC-Council specialists.

To become certified in ECIH v2, candidates must pass a rigorous certification exam that tests their knowledge, skills, and abilities in the areas of incident handling and response. 212-89 Exam consists of 100 multiple-choice questions, and candidates have 3 hours to complete the exam. 212-89 exam is designed to test the candidate's knowledge of incident handling and response techniques, as well as their ability to analyze and respond to security incidents.

>> Test 212-89 Testking <<

Test 212-89 Testking offer you accurate Best Vce to pass EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) exam

After the advent of the TestSimulate's latest EC-COUNCIL certification 212-89 exam practice questions and answers, passing EC-COUNCIL certification 212-89 exam is no longer a dream of the IT staff. All of TestSimulate's practice questions and answers about EC-COUNCIL Certification 212-89 Exam have high quality and 95% similarity with the real exam questions. TestSimulate is worthful to choose. If you choose TestSimulate's products, you will be well prepared for EC-COUNCIL certification 212-89 exam and then successfully pass the exam.

The EC Council Certified Incident Handler (ECIH v2) certification exam is a highly respected certification in the field of cybersecurity. EC Council Certified Incident Handler (ECIH v3) certification is designed to demonstrate an individual’s ability to handle and respond to various types of cybersecurity incidents, including network security incidents, application security incidents, and cloud security incidents. EC Council Certified Incident Handler (ECIH v3) certification exam covers a range of topics, including incident handling process, incident response teams, and forensic analysis.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q273-Q278):

NEW QUESTION # 273
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. Eradication - Containment - Identification - Preparation - Recovery - Follow-up
- C. Identification - Preparation - Containment - Recovery - Follow-up - Eradication
- D. Preparation - Identification - Containment - Eradication - Recovery - Follow-upà

Answer: D

NEW QUESTION # 274
Eric who is an incident responder is working on developing incident-handling plans and procedures. As part of this process, he is performing analysis on the organizational network to generate a report and to develop policies based on the acquired results.
Which of the following tools will help him in analyzing network and its related traffic?

- A. Whois
- B. Wireshark
- C. FaceNiff
- D. Burp Suite

Answer: B

NEW QUESTION # 275
Which of the following is a volatile evidence collecting tool?

- A. Hash Tool
- B. FTK Images
- C. Pro Discover Forensics
- D. Netstat

Answer: D

NEW QUESTION # 276
A national research agency was recently subjected to a comprehensive cybersecurity compliance audit.
During the audit, reviewers evaluated how the agency's incident response unit manages harmful code samples during investigations. The assessment revealed that team members often interacted with dangerous file payloads directly on enterprise-connected systems used for general operations. Furthermore, no precautionary renaming was applied to prevent accidental triggering, and sensitive materials were placed in areas accessible by non-specialized personnel. The auditors flagged these practices as severely noncompliant with safe sample processing protocols and recommended urgent changes to prevent operational fallout or accidental outbreaks.
Which best practice for secure handling of malicious code was most clearly disregarded in this case?

- A. Create vulnerability documentation for each malware sample to support threat profiling and archival.
- B. Storing malware samples with non-executable file extensions in isolated environments.
- C. Tagging malware sample files with platform-specific behavior indicators for improved categorization.
- D. Encrypting all malware sample files using symmetric encryption.

Answer: B

Explanation:
Comprehensive and Detailed Explanation (ECIH-aligned):
This scenario highlights violations of forensic readiness and safe malware handling, which are explicitly covered in the ECIH First Response and Malware Analysis modules. ECIH stresses that malware samples must never be handled on production or enterprise-connected systems, as this creates a high risk of accidental execution, lateral infection, and organizational impact.
Option A is correct because ECIH mandates that malicious code samples be stored in isolated, non- networked environments and renamed with non-executable extensions (for example, .malware, .bin, or .txt) to prevent accidental execution. This practice ensures operational safety and preserves forensic integrity.
Option B improves confidentiality but does not prevent accidental execution. Option C supports documentation but does not mitigate execution risk. Option D aids classification but does not address safe handling.
The described behavior-handling live malware on enterprise systems without isolation or renaming- directly contradicts ECIH best practices. Proper sample isolation, renaming, and access restriction are mandatory controls to prevent secondary incidents during investigations, making Option A the correct answer.

NEW QUESTION # 277

Ross is an incident manager (IM) at an organization, and his team provides support to all users in the organization who are affected by threats or attacks. David, who is the organization's internal auditor, is also part of Ross's incident response team. Which of the following is David's responsibility?

- A. Coordinate incident containment activities with the information security officer (ISO).
- B. Configure information security controls.
- C. Identify and report security loopholes to the management for necessary action.
- D. Perform the- necessary action to block the network traffic from the suspectoc intruder.

Answer: C

Explanation:
In the context of an incident response team, the role of an internal auditor like David includes identifying, evaluating, and reporting on information security risks and vulnerabilities within the organization. His responsibility is to ensure that the organization's security controls are effective and to identify any security loopholes that could be exploited by attackers. Once identified, he reports these vulnerabilities to management so that they can take the necessary actions to mitigate the risks. This role is critical in maintaining theorganization's overall security posture and ensuring compliance with relevant laws, regulations, and policies.
References:Incident Handler (ECIH v3) courses and study guides cover the roles and responsibilities of incident response team members, highlighting the importance of internal auditors in identifying and addressing security vulnerabilities.

NEW QUESTION # 278
.....