Pass Guaranteed 2026 212-89: Efficient Dumps EC Council Certified Incident Handler (ECIH v3) Vce

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

Our 212-89 preparation torrent can keep pace with the digitized world by providing timely application. There are versions of Software and APP online, they can simulate the real exam environment. If you take good advantage of this 212-89 practice materials character, you will not feel nervous when you deal with the 212-89 Real Exam. Furthermore, they can be downloaded to all electronic devices so that you can have a rather modern study experience conveniently. Why not have a try on our 212-89 exam questions?

EC-COUNCIL 212-89 Exam is a certification program designed for professionals in the field of incident handling and response. EC Council Certified Incident Handler (ECIH v3) certification is globally recognized and is considered one of the most prestigious certifications in the field of cybersecurity. The EC-COUNCIL 212-89 exam is also known as the EC Council Certified Incident Handler (ECIH v2) certification exam.

The EC-Council 212-89 exam measures the knowledge and competence of the candidates in identifying, analyzing, and rectifying hazards to prevent any future reoccurrences. The interested individuals who pass this certification test will gain the fundamental skills in responding and handling computer security incidents within an information system. A certified applicant is a skilled professional with the ability to handle different incident types, risk assessment methodologies, as well as different policies and laws associated with incident handling. So, if you want to become one of these experts, you will need to know a lot of details.

>> Dumps 212-89 Vce <<

2026 Dumps 212-89 Vce | Newest 212-89 100% Free Real Brain Dumps

In order to make sure your whole experience of buying our 212-89 study materials more comfortable, our company will provide all people with 24 hours online service. The experts and professors from our company designed the online service system for all customers. If you decide to buy the 212-89 Study Materials from our company, we can make sure that you will have the opportunity to enjoy the best online service provided by our excellent online workers.

The EC-Council Certified Incident Handler (ECIH) certification exam is intended for security professionals who want to validate

their skills and knowledge in incident handling and response. The ECIH certification exam is based on the latest version of the ECIH v2 courseware, which covers a wide range of topics related to incident handling and response. 212-89 Exam is a 2-hour, computer-based exam that consists of 100 multiple-choice questions, and an individual must score at least 70% on the exam to pass.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q190-Q195):

NEW QUESTION # 190
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 the agency's reporting timeframe guidelines, this incident should be reported within 2h of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate the activity.
Which incident category of US Federal Agency does this incident belong to?

- A. CAT 6
- B. CAT 1
- C. CAT 5
- D. CAT 2

Answer: D

NEW QUESTION # 191
CSIRT can be implemented at:

- A. All the above
- B. Vendor level
- C. Internal enterprise level
- D. National, government and military level

Answer: A

NEW QUESTION # 192
Alice is an incident handler and she has been informed by her lead that the data on affected systems must be backed up so that it can be retrieved if it is damaged during the incident response process. She was also told that the system backup can also be used for further investigation of the incident. In which of the following stages of the incident handling and response (IH&R) process does Alice need to do a complete backup of the infected system?

- A. Containment
- B. Eradication
- C. Incident recording
- D. Incident triage

Answer: A

Explanation:
In the incident handling and response (IH&R) process, backing up the data on affected systems is a critical step that usually falls under the Containment phase. The Containment phase is crucial for limiting the scope and severity of an incident, ensuring that it does not spread further or affect additional systems. Backing up affected systems during containment is essential for several reasons: it preserves a snapshot of the system in its current state for forensic analysis, ensures that data is not lost if the system needs to be wiped or altered during the response process, and helps in the recovery process if data is corrupted or lost.
By performing a complete backup of the infected system during the Containment phase, Alice ensures that there is a reliable copy of all data and system states before any major actions, such as eradication or deeper forensic analysis, are taken. This step is also preparatory for the potential use of the backup in analyzing how the incident occurred and in restoring system functionality after the incident is resolved.
References:EC-Council's Certified Incident Handler (ECIH v3) courses and study guides highlight the importance of the Containment phase in the IH&R process, including the practice of backing up affected systems to prevent data loss and to aid in the investigation and recovery processes.

NEW QUESTION # 193
A cybersecurity analyst at a technology firm discovers suspicious activity on a network segment dedicated to research and development. The initial indicators suggest a possible compromise of several endpoints with potential intellectual property theft. Given the sensitive nature of the data involved, what is the most effective method for the analyst to detect and validate the security incident?

- A. Conduct a network-wide vulnerability scan.
- B. Immediately notify law enforcement and regulatory bodies.
- C. Deploy an endpoint detection and response (EDR) solution to identify and investigate suspicious activities.
- D. Isolate the affected network segment and manually inspect each endpoint.

Answer: C

Explanation:
Comprehensive and Detailed Explanation (ECIH-aligned):
The ECIH Endpoint Security module stresses that modern endpoint incidents require advanced detection capabilities beyond traditional antivirus or manual inspection. Intellectual property theft often involves stealthy techniques that evade basic controls.
Option C is correct because an Endpoint Detection and Response (EDR) solution provides deep visibility into endpoint behavior, including process execution, memory activity, file changes, and lateral movement. EDR enables analysts to detect, investigate, and validate incidents efficiently across multiple endpoints.
Option B is slow and error-prone. Option A is premature without validation. Option D identifies vulnerabilities, not active compromise.
ECIH highlights EDR as a cornerstone technology for endpoint incident detection and validation, especially in high-value environments such as R&D networks.

NEW QUESTION # 194
During the vulnerability assessment phase, the incident responders perform various steps as below:
1. Run vulnerability scans using tools
2. Identify and prioritize vulnerabilities
3. Examine and evaluate physical security
4. Perform OSINT information gathering to validate the vulnerabilities
5. Apply business and technology context to scanner results
6. Check for misconfigurations and human errors
7. Create a vulnerability scan report
Identify the correct sequence of vulnerability assessment steps performed by the incident responders.

- A. 1-->3-->2-->4-->5-->6-->7
- B. 2-->1-->4-->7-->5-->6-->3
- C. 4-->1-->2-->3-->6-->5-->7
- D. 3-->6-->1-->2-->5-->4-->7

Answer: C

Explanation:
The correct sequence of steps performed by incident responders during the vulnerability assessment phase is as follows:
* Perform OSINT information gathering to validate the vulnerabilities (4):Initially, Open Source Intelligence (OSINT) is used to gather information about the organization's digital footprint and potential vulnerabilities.
* Run vulnerability scans using tools (1):Next, specialized tools are employed to scan the organization's networks and systems for vulnerabilities.
* Identify and prioritize vulnerabilities (2):The identified vulnerabilities are then analyzed and prioritized based on their severity and potential impact on the organization.
* Examine and evaluate physical security (3):Physical security assessments are also crucial as they can impact the overall security posture and protection of digital assets.
* Check for misconfigurations and human errors (6):This step involves looking for misconfigurations in systems and networks, as well as potential human errors that could lead to vulnerabilities.
* Apply business and technology context to scanner results (5):The results from the scans are evaluated within the context of the business and its technology environment to accurately assess risks.
* Create a vulnerability scan report (7):Finally, a comprehensive report is created, detailing the vulnerabilities, their severity, and recommended mitigation strategies.
This sequence ensures a thorough assessment, prioritizing vulnerabilities that pose the greatest risk and providing actionable insights

for mitigation.
References:ECIH v3 courses and study guides elaborate on the vulnerability assessment process, detailing the steps involved in identifying, evaluating, and addressing security vulnerabilities within an organization's IT infrastructure.

NEW QUESTION # 195
.....