100% Pass Quiz The Best 212-89 - EC Council Certified Incident Handler (ECIH v3) Latest Test Sample

P.S. Free 2026 EC-COUNCIL 212-89 dumps are available on Google Drive shared by Getcertkey: https://drive.google.com/open?id=1Hpc9QVXGbIWtLg2ej0sl8EvW_Rx1V7as

Our EC-COUNCIL 212-89 qualification test help improve your technical skills and more importantly, helping you build up confidence to fight for a bright future in tough working environment. Our professional experts devote plenty of time and energy to developing the 212-89 Study Tool. You can trust us and let us be your honest cooperator in your future development. Here are several advantages about our EC-COUNCIL 212-89 exam for your reference.

The ECIH v2 certification exam is a multiple-choice exam that consists of 100 questions. 212-89 exam duration is four hours, and candidates must score at least 70% to pass the exam. 212-89 Exam is computer-based and is administered at authorized testing centers worldwide.

>> 212-89 Latest Test Sample <<

212-89 Latest Test Sample - Pass Guaranteed Quiz First-grade EC-COUNCIL Examcollection 212-89 Free Dumps

To meet the different and specific versions of consumers, and find the greatest solution to help you review, we made three versions for you. Three versions of EC Council Certified Incident Handler (ECIH v3) prepare torrents available on our test platform, including PDF version, PC version and APP online version. The trait of the software version is very practical. It can simulate real test environment, you can feel the atmosphere of the EC Council Certified Incident Handler (ECIH v3) exam in advance by the software version, and install the software version several times. PDF version of 212-89 Exam torrents is convenient to read and remember, it also can be printed into papers so that you are able to write some notes or highlight the emphasis. PC version of our 212-89 test braindumps only supports windows users and it is also one of our popular types to choose.

EC-COUNCIL 212-89 (EC Council Certified Incident Handler (ECIH v2)) certification exam is designed for professionals who want to gain knowledge and skills in incident handling and response. EC Council Certified Incident Handler (ECIH v3) certification is recognized globally and is considered one of the most prestigious certifications in the information security industry. 212-89 Exam is based on real-world scenarios and focuses on technical and practical skills rather than just theoretical knowledge.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q46-Q51):

NEW QUESTION # 46
The sign of incident that may happen in the future is called:

- A. A Reactive
- B. A Precursor
- C. An Indication
- D. A Proactive

Answer: B

NEW QUESTION # 47
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

NEW QUESTION # 48
In an international bank, the IT security team identified unusual network traffic indicating a potential malware infection. Further analysis revealed that several high-value transaction servers were communicating with an external command and control server. The team needs to decide the immediate action to best handle this malware incident triage. What should they prioritize to mitigate the threat and safeguard sensitive data effectively?

- A. Initiating a controlled shutdown of the transaction servers to preserve their current state
- B. Immediately updating antivirus signatures on all network devices and servers
- C. Performing a memory dump of the affected servers for in-depth forensic analysis
- D. Disconnecting the affected servers from the network to prevent further data exfiltration

Answer: D

Explanation:
Comprehensive and Detailed Explanation (ECIH-aligned):
This scenario describes an active malware infection with confirmed command-and-control (C2) communication, which represents an immediate and severe risk to sensitive financial data. According to the EC-Council ECIH malware incident handling process, the first priority in such cases is containment, specifically stopping ongoing malicious activity and preventing further data exfiltration.
Option A is correct because disconnecting the affected servers from the network immediately severs the attacker's control channel and halts outbound data leakage. ECIH emphasizes that when C2 traffic is observed, responders must act decisively to isolate compromised systems before pursuing deeper forensic analysis or remediation. Containment minimizes damage and reduces legal, financial, and reputational impact.
Option B may preserve system state but allows continued exfiltration until shutdown is complete and may disrupt critical banking operations. Option C is a preventive measure and does not stop an active infection.
Option D is valuable for investigation but should occur after containment, not before.
ECIH guidance consistently prioritizes stopping harm over gathering evidence when critical assets are at risk.
Therefore, immediate network disconnection of affected servers is the correct triage action.

NEW QUESTION # 49
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. Within four (4) hours of discovery/detection if the successful attack is still ongoing and agency is unable to

successfully mitigate activity

- B. Within two (2) hours of discovery/detection
- C. Weekly
- D. Monthly

Answer: C

NEW QUESTION # 50
According to US-CERT; if an agency is unable to successfully mitigate a DOS attack it must be reported within:

- A. One (1) hour of discovery/detection if the successful attack is still ongoing
- B. Four (4) hours of discovery/detection if the successful attack is still ongoing
- C. Three (3) hours of discovery/detection if the successful attack is still ongoing
- D. Two (2) hours of discovery/detection if the successful attack is still ongoing

Answer: D

NEW QUESTION # 51
.....

2026 Latest Getcertkey 212-89 PDF Dumps and 212-89 Exam Engine Free Share: https://drive.google.com/open?id=1Hpc9QVXGblWtLg2ej0sl8EvW_Rx1V7as