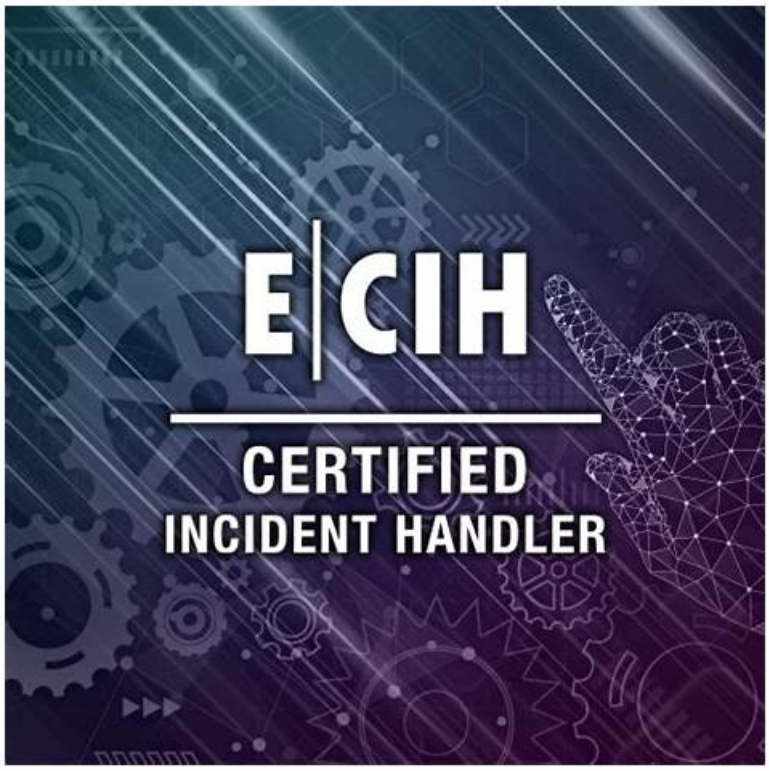
212-89 Preparation Materials and 212-89 Study Guide: EC Council Certified Incident Handler (ECIH v3) Real Dumps



What's more, part of that BraindumpsIT 212-89 dumps now are free: https://drive.google.com/open?id=1gTua8L9Zg4MKuQwKsc56MsvTpXlDHedB

Our company has always been following the trend of the 212-89 certification. Our research and development team not only study what questions will come up in the 212-89 exam, but also design powerful study tools like exam simulation software. With the Software version of our 212-89 study materilas, you can have the experience of the real exam which is very helpful for some candidates who lack confidence or experice of our 212-89 training guide.

However, you should keep in mind that to get success in the 212-89 certification exam is not a simple and easy task. A lot of effort, commitment, and in-depth EC Council Certified Incident Handler (ECIH v3) (212-89) exam questions preparation is required to pass this 212-89 Exam. For the complete and comprehensive EC Council Certified Incident Handler (ECIH v3) (212-89) exam dumps preparation you can trust valid, updated, and 212-89 Questions which you can download from the BraindumpsIT platform quickly and easily.

>> Reliable 212-89 Test Forum <<

212-89 Study Dumps - VCE 212-89 Exam Simulator

Actual and updated 212-89 questions are essential for individuals who want to clear the 212-89 examination in a short time. At BraindumpsIT, we understand that the learning style of every 212-89 exam applicant is different. That's why we offer three formats of EC-COUNCIL 212-89 Dumps. With our actual and updated 212-89 questions, you can achieve success in the EC-COUNCIL Certification Exam and accelerate your career on the first attempt.

EC-COUNCIL 212-89 Exam covers a wide range of topics, including incident handling process, risk management, computer forensics, and network security essentials. 212-89 exam is designed to test the candidate's ability to identify, respond to, and resolve security incidents in a timely and effective manner. EC Council Certified Incident Handler (ECIH v3) certification is valid for three years, and candidates must renew their certification after that period to keep up with the latest trends and technologies in incident handling and response.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q95-Q100):

NEW QUESTION # 95
During the process of detecting and containing malicious emails, incident responders should examine the originating IP address of the emails.
The steps to examine the originating IP address are as follow:
1. Search for the IP in the WHOIS database
2. Open the email to trace and find its header
3. Collect the IP address of the sender from the header of the received mail
4. Look for the geographic address of the sender in the WHOIS database
Identify the correct sequence of steps to be performed by the incident responders to examine originating IP address of the emails.

- A. 2-->1-->4-->3
- B. 1-->3-->2-->4
- C. 4-->1-->2-->3
- D. 2-->3-->1-->4

Answer: D

NEW QUESTION # 96
Which of the following is defined as the identification of the boundaries of an IT system along with the resources and information that constitute the system?

- A. Control analysis
- B. System characterization
- C. Vulnerability identification
- D. Threat identification

Answer: B

NEW QUESTION # 97
Agencies do NOT report an information security incident is because of:

- A. Afraid of negative publicity
- B. Have full knowledge about how to handle the attack internally
- C. Do not want to pay the additional cost of reporting an incident
- D. All the above

Answer: A

NEW QUESTION # 98
Which of the following is a common tool used to help detect malicious internal or compromised actors?

- A. Syslog configuration
- B. SOC2 compliance report
- C. User behavior analytics
- D. Log forward ng

Answer: C

Explanation:
User Behavior Analytics (UBA) is a cybersecurity process or tool that utilizes machine learning, algorithms, and statistical analyses to detect potentially harmful activities within an organization's network by comparing them against established patterns of users' behavior. It is particularly effective in identifying malicious internal actors or compromised users who may be conducting activities that deviate from their normal behavior patterns, such as accessing unauthorized data or systems, excessive file downloads, or unusual login times. UBA tools can flag these activities for further investigation, often before traditional security tools detect a breach.

In contrast, SOC2 compliance reports, log forwarding, and syslog configuration are important for maintaining and auditing security standards and for infrastructure monitoring, but they are not primarily focused on detecting malicious behavior based on deviations from established user behavior patterns.
References:The Incident Handler (ECIH v3) curriculum discusses various tools and methodologies for detecting and responding to security incidents, highlighting User Behavior Analytics as a key tool for identifying insider threats and compromised accounts through behavioral monitoring and analysis.

NEW QUESTION # 99
Clark is investigating a cybercrime at TechSoft Solutions. While investigating the case, he needs to collect volatile information such as running services, their process IDs, startmode, state, and status.
Which of the following commands will help Clark to collect such information from running services?

- A. net file
- B. netstat -ab
- C. wmic
- D. Openfiles

Answer: D

Explanation:
WMIC (Windows Management Instrumentation Command-line) is a command-line tool that provides a unified interface for Windows management tasks, including the collection of system information. It allows administrators and forensic investigators to query the live system for information about running services, their process IDs, start modes, states, and statuses, among other data. The use of WMIC is particularly valuable in incident response scenarios for gathering volatile information from a system without having to install additional software, which might alter the state of the system being investigated. By executing specific WMIC commands, Clark can extract detailed information about the services running on a system at the time of the investigation, making it an essential tool for collecting volatile data in a forensically sound manner.
References:The ECIH v3 courses and study guides emphasize the importance of collecting volatile data during incident response and digital forensics investigations. They specifically highlight the use of built-in Windows tools like WMIC for gathering essential system information without compromising the integrity of the evidence.

NEW QUESTION # 100
.....

for 【 212-89 】 and easily obtain a free download on ➤ www.dumps4pdf.com □ □212-89 Practice Exam Fee

- New Launch 212-89 EC Council Certified Incident Handler (ECIH v3) Dumps Options To Pass the Exam 2025 □ Simply search for ➡ 212-89 □□□ for free download on ▸ www.pdfvce.com ◂ □Dumps 212-89 Vce
- 212-89 Practice Exam Fee ♥ 212-89 Practice Exam Fee □ 212-89 Valid Braindumps Questions □ Search for ⇛ 212-89 ⇚ and obtain a free download on 《 www.free4dump.com 》 □212-89 Latest Test Bootcamp
- lifepass.site, lt.dananxun.cn, www.eabook.cn, 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, lineage95003.官網.com, lms.ait.edu.za, paraschessacademy.com, nalogi-v-germanii.de, dulanonline.com, 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, Disposable vapes

BTW, DOWNLOAD part of BraindumpsIT 212-89 dumps from Cloud Storage: https://drive.google.com/open?id=1gTua8L9Zg4MKuQwKsc56MsvTpXlDHedB