Related EC-COUNCIL 212-89 Certifications - Exam 212-89 Objectives Pdf

2026 Latest Test4Sure 212-89 PDF Dumps and 212-89 Exam Engine Free Share: https://drive.google.com/open?id=1AZlldF6jwe4LFcOyHPxuN7bHggfwVnZS

Test4Sure have made sure that each EC-COUNCIL 212-89 exam questions are updated according to the latest EC-COUNCIL 212-89 exam criteria issued by EC-COUNCIL. Each EC-COUNCIL 212-89 exam question gets reviewed by EC-COUNCIL professionals many times to ensure incomparable accuracy. Test4Sure offer a demo version of the actual EC-COUNCIL 212-89 Exam Question only for customer satisfaction and the candidates can check the validity of the product before actually buying it.

The EC-Council Certified Incident Handler (ECIH v2) certification is designed to equip professionals with the necessary skills to detect, respond, and manage computer security incidents effectively. The ECIH certification is globally recognized as a benchmark for incident handling and response training, and it validates the knowledge and skills required to manage and respond to various types of security incidents, including network security incidents, malware incidents, and insider threats. EC Council Certified Incident Handler (ECIH v3) certification is highly sought after by employers as it demonstrates that the certified professional has the knowledge and skills required to handle and respond to security incidents in a timely and effective manner.

>> Related EC-COUNCIL 212-89 Certifications <<

Exam 212-89 Objectives Pdf & Pdf 212-89 Braindumps

Of course, when we review a qualifying exam, we can't be closed-door. We should pay attention to the new policies and information related to the test 212-89 certification. For the convenience of the users, the 212-89 test materials will be updated on the homepage and timely update the information related to the qualification examination. Annual qualification examination, although content broadly may be the same, but as the policy of each year, the corresponding examination pattern grading standards and hot spots will be changed, the 212-89 Test Prep can help users to spend the least time to pass the exam.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q213-Q218):

NEW QUESTION # 213
Adam is an incident handler who intends to use DBCC LOG command to analyze a database and retrieve the active transaction log files for the specified database. The syntax of DBCC LOG command is DBCC LOG(,), where the output parameter specifies the level of information an incident handler wants to retrieve. If Adam wants to retrieve the full information on each operation along with the hex dump of a current transaction row, which of the following output parameters should Adam use?

- A. 0
- B. 1
- C. 2
- D. 3

Answer: C

Explanation:
The DBCC LOG command is used in SQL Server environments to analyze the transaction log files of a database. It provides insights into the transactions that have occurred, which is crucial for forensic analysis in the event of an incident. The syntaxDBCC LOG(<database_name>, <output_level>)allows an incident handler to specify the level of detail they wish to retrieve from the log files. When an incident handler like Adam requires the full information on each operation along with the hex dump of the current transaction row, the output parameter should be set to 4. This level of output is the most verbose, providing comprehensive details about each transaction, including a hex dump which is essential for a deep forensic analysis. It helps in understanding the exact changes made by transactions, which can be pivotal in investigating incidents involving data manipulation or other unauthorized database activities.
References:EC-Council's Certified Incident Handler (ECIH v3) program emphasizes the importance of understanding and utilizing various tools and commands for forensic analysis, including how to use the DBCC LOG command for transaction log analysis in SQL Server environments.

NEW QUESTION # 214
Ensuring the integrity, confidentiality and availability of electronic protected health information of a patient is known as:

- A. Social Security Act
- B. Sarbanes-Oxley Act
- C. Gramm-Leach-Bliley Act
- D. Health Insurance Portability and Privacy Act

Answer: D

NEW QUESTION # 215
Which of the following GPG18 and Forensic readiness planning (SPF) principles states that "organizations should adopt a scenario based Forensic Readiness Planning approach that learns from experience gained within the business"?

- A. Principle 3
- B. Principle 5
- C. Principle 7
- D. Principle 2

Answer: B

Explanation:
The GPG18 and Forensic readiness planning (SPF) principles outline various guidelines to enhance an organization's readiness for forensic investigation and response. Principle 5, which suggests that organizations should adopt a scenario-based Forensic Readiness Planning approach that learns from experience gained within the business, emphasizes the importance of being prepared for a wide range of potential incidents by leveraging lessons learned from past experiences. This approach helps in continuously improving forensic readiness and response capabilities by adapting to the evolving threat landscape and organizational changes.
References:While specific documentation from GPG18 and SPF might detail these principles, the ECIH v3 program by EC-Council covers the concept of forensic readiness planning, including adopting scenario-based approaches and learning from past incidents as a fundamental aspect of enhancing an organization's incident response and forensic capabilities.

NEW QUESTION # 216
A multinational corporation with a diverse computing environment experiences a sophisticated malware attack targeting its endpoint devices. The malware is designed to evade traditional antivirus solutions and establish a persistent backdoor for data exfiltration. This incident underscores the complex landscape of endpoint security and the evolving threat vectors. In this context, what is the most critical reason for establishing a robust endpoint security incident handling and response capability?

- A. To ensure compliance with international data protection regulations.
- B. To enable rapid containment and eradication of threats to maintain business continuity.
- C. To mitigate financial losses associated with data breaches and system downtime.
- D. To facilitate real-time threat intelligence sharing across the industry.

Answer: B

Explanation:

The primary objective of endpoint incident handling, as outlined in the ECIH curriculum, is rapid containment and eradication of threats to preserve business operations. Advanced malware that bypasses traditional defenses requires coordinated response capabilities to prevent widespread compromise.
Option D is correct because endpoint IH&R enables organizations to quickly isolate infected systems, remove malicious components, and restore trusted states, thereby maintaining operational continuity. ECIH emphasizes speed and coordination as critical success factors in endpoint response.
Option A is secondary. Option B is a compliance outcome, not a response objective. Option C is a consequence, not the primary driver.
Therefore, the most critical reason is to ensure rapid containment and eradication, making Option D correct.

NEW QUESTION # 217
Which of the following is an Inappropriate usage incident?

- A. Denial-of-service attack
- B. Insider threat
- C. Reconnaissance attack
- D. Access-control attack

Answer: B

Explanation:
An Inappropriate Usage incident refers to instances where computing resources are misused or abused, often violating organizational policies or laws. While access-control attacks, reconnaissance attacks, and denial-of- service (DoS) attacks represent different types of external threats or methods of attack, an Insider Threat is an example of inappropriate usage. Insider threats come from individuals within the organization, such as employees or contractors, who misuse their access to harm the organization's interests. This can include stealing confidential information, intentionally disrupting systems, or other malicious activities that leverage their legitimate access to the organization's resources.
References:EC-Council's Incident Handler (ECIH v3) materials often discuss various types of security incidents, including inappropriate usage, and emphasize the importance of recognizing and preparing for insider threats as a critical component of an organization's incident response strategy.

NEW QUESTION # 218
.....

Infinite striving to be the best is man's duty. We have the responsibility to realize our values in the society. Of course, you must have enough ability to assume the tasks. Then our 212-89 learning quiz can give you some help. First of all, you can easily pass the 212-89 Exam and win out from many candidates for our 212-89 study materials are the most effective exam materials in the market. Secondly, you can also learn a lot of the specilized knowledage at the same time.

www.examcollectionpass.com ） is best website to obtain ➠ 212-89 □ for free download □212-89 Exam Labs

- 212-89 Latest Braindumps Files ↗ 212-89 Accurate Prep Material □ 212-89 Accurate Prep Material □ Search on ➡ www.pdfvce.com □□□ for （ 212-89 ） to obtain exam materials for free download □Latest 212-89 Test Blueprint
- 100% Pass Quiz 2026 EC-COUNCIL 212-89 – Valid Related Certifications □ Search for ➤ 212-89 □ and download exam materials for free through ➡ www.exam4labs.com □□□ □212-89 Clear Exam
- 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, www.stes.tyc.edu.tw, minalcze148368.jasperwiki.com, wzsj.lwtcc.cn, lexievkid125429.blogchaat.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, janadqtm386177.blog5star.com, esmeedphx299467.blogitright.com, ez-bookmarking.com, tornadosocial.com, Disposable vapes

What's more, part of that Test4Sure 212-89 dumps now are free: https://drive.google.com/open?id=1AZlldF6jwe4LFcOyHPxuN7bHggfwVnZS