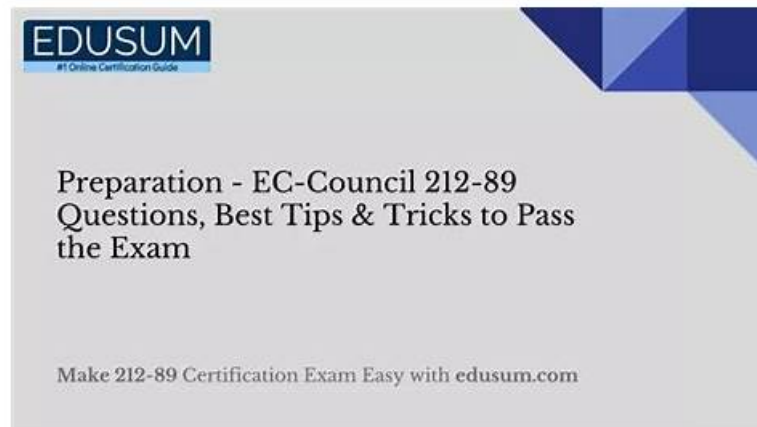


# Here's The Proven And Quick Way To Get Success In EC-COUNCIL 212-89 Exam



P.S. Free 2025 EC-COUNCIL 212-89 dumps are available on Google Drive shared by PDF4Test: <https://drive.google.com/open?id=1APJ6CEZ2pZkZD42BQAGm0uiMlkQPw7cl>

Our 212-89 training materials have won great success in the market. Tens of thousands of the candidates are learning on our 212-89 practice engine. First of all, our 212-89 study dumps cover all related tests about computers. It will be easy for you to find your prepared learning material. If you are suspicious of our 212-89 Exam Questions, you can download the free demo from our official websites.

The ECIH v2 certification is an important credential for IT security professionals who are involved in incident handling and response. EC Council Certified Incident Handler (ECIH v3) certification demonstrates that the candidate has the knowledge, skills, and abilities to effectively manage and respond to security incidents. It also provides employers with a way to evaluate the skills of their IT security staff, and to ensure that they have the necessary expertise to protect their organization's critical assets.

>> Valid 212-89 Exam Testking <<

## Accurate Valid 212-89 Exam Testking bring you Effective Reliable 212-89 Test Topics for EC-COUNCIL EC Council Certified Incident Handler (ECIH v3)

PDF4Test IT Certification has years of training experience. PDF4Test EC-COUNCIL 212-89 exam training materials is a reliable product. IT elite team continue to provide our candidates with the latest version of the 212-89 exam training materials. Our staff made great efforts to ensure that you always get good grades in examinations. To be sure, PDF4Test EC-COUNCIL 212-89 Exam Materials can provide you with the most practical IT certification material.

## EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q89-Q94):

### NEW QUESTION # 89

Sam, an employee of a multinational company, sends emails to third-party organizations with a spoofed email address of his organization. How can you categorize this type of incident?

- A. Network intrusion incident
- B. Denial-of-service incident
- C. Unauthorized access incident.
- D. Inappropriate usage incident

**Answer: D**

**Explanation:**

An inappropriate usage incident involves misuse of the organization's resources or violations of its acceptable use policies. Sam's

actions, where he sends emails to third-party organizations with a spoofed email address of his employer, constitute misuse of the organization's email system and misrepresentation of the organization.

This behavior can harm the organization's reputation, violate policy, and potentially lead to legal consequences. Inappropriate usage incidents can range from unauthorized use of systems for personal gain to the dissemination of unapproved content.

References: The Incident Handler (ECIH v3) by EC-Council includes discussions on various types of security incidents, emphasizing the importance of addressing and mitigating not just external threats but also internal misuse and policy violations.

#### NEW QUESTION # 90

Your company sells SaaS, and your company itself is hosted in the cloud (using it as a PaaS). In case of a malware incident in your customer's database, who is responsible for eradicating the malicious software?

- A. Your company
- B. Building management
- C. The PaaS provider
- D. The customer

**Answer: A**

Explanation:

In the scenario where your company sells Software as a Service (SaaS) and is hosted on the cloud using it as a Platform as a Service (PaaS), your company is responsible for eradicating malware in your customer's database. This is because, as the SaaS provider, your company manages the software and is responsible for its security and maintenance, including the databases that store customer data. While the PaaS provider is responsible for the underlying infrastructure, platform, and possibly some middleware security aspects, the application layer security, including data and application management, falls to the SaaS provider. Building management would not be involved in digital security matters, and while customers are responsible for their data, the actual software maintenance and security in a SaaS model are the provider's responsibility.

References: Incident Handler (ECIH v3) certification materials often discuss cloud service models (IaaS, PaaS, SaaS) and their associated security responsibilities, highlighting the importance of understanding who is responsible for what in cloud environments.

#### NEW QUESTION # 91

Jason is setting up a computer forensics lab and must perform the following steps: 1. physical location and structural design considerations; 2. planning and budgeting; 3. work area considerations; 4. physical security recommendations; 5. forensic lab licensing; 6. human resource considerations. Arrange these steps in the order of execution.

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

**Answer: D**

Explanation:

Setting up a computer forensics lab involves several critical steps that need to be executed in a logical and efficient order. The correct sequence starts with planning and budgeting(2), as it is essential to understand the scope, resources, and financial commitment required for the lab. The next step involves considering the physical location and structural design (1) to ensure the lab meets operational needs and security requirements.

Work area considerations (3) follow, focusing on the layout and functionality of the workspace. Human resource considerations (6) are crucial next, to ensure the lab is staffed with qualified personnel. Physical security recommendations (4) are then implemented to protect the lab and its resources. Finally, forensic lab licensing (5) ensures the lab operates within legal and regulatory frameworks.

References: The ECIH v3 course materials from EC-Council outline the foundational steps for setting up a computer forensics lab, stressing the importance of thorough planning and adherence to best practices in lab design and operation.

#### NEW QUESTION # 92

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

**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 # 93

Which of the following processes is referred to as an approach to respond to the security incidents that occurred in an organization and enables the response team by ensuring that they know exactly what process to follow in case of security incidents?

- A. Risk assessment
- **B. Incident response orchestration**
- C. Vulnerability management
- D. Threat assessment

**Answer: B**

Explanation:

Incident response orchestration refers to the process and technologies used to coordinate and streamline the response to security incidents. This approach ensures that incident response teams have clear procedures and workflows to follow, enabling them to act swiftly and effectively when dealing with security incidents. By orchestrating the response, organizations can minimize the impact of incidents, ensure consistent and thorough investigation and remediation activities, and improve their overall security posture. Incident response orchestration involves integrating various security tools, automating response actions where possible, and providing a centralized platform for managing incidents.

References: The concept of incident response orchestration and its role in enhancing the effectiveness of incident handling and response efforts is discussed in cybersecurity literature and training, including ECIH v3 study materials, which highlight the benefits of having a structured and organized approach to managing security incidents.

### NEW QUESTION # 94

.....

In your day-to-day life, things look like same all the time. Sometimes you feel the life is so tired, do the same things again and again every day. Doing the same things and living on the same life make you very bored. So hurry to prepare for 212-89 exam, we believe that our 212-89 exam braindumps will help you change your present life. It is possible for you to start your new and meaningful life in the near future, if you can pass the EC-COUNCIL exam and get the certification. So it is very important for you to prepare for the practice exam, you must pay more attention to the 212-89 Certification guide to help you.

**Reliable 212-89 Test Topics:** <https://www.pdf4test.com/212-89-dump-torrent.html>

- Latest 212-89 Reliable Torrent - 212-89 Actual Pdf - 212-89 Exam Questions □ [ [www.dumpsquestion.com](http://www.dumpsquestion.com) ] is best website to obtain ⇒ 212-89 ⇐ for free download □ 212-89 Clearer Explanation
- Free PDF EC-COUNCIL - 212-89 - EC Council Certified Incident Handler (ECIH v3) –The Best Valid Exam Testking □ □ Search for 《 212-89 》 and download exam materials for free through “ [www.pdfvce.com](http://www.pdfvce.com) ” □ Books 212-89 PDF
- 212-89 Valid Test Pass4sure □ Test 212-89 Free □ PdfDemo 212-89 Download □ Copy URL ☀ [www.testkingpdf.com](http://www.testkingpdf.com) □ ☀ □ open and search for “212-89 ” to download for free □ 212-89 Pdf Dumps
- 212-89 Clearer Explanation □ Latest 212-89 Exam Preparation □ 212-89 Valid Test Pass4sure □ Simply search for

- 《 212-89 》 for free download on ➡ [www.pdfvce.com](http://www.pdfvce.com) ☐ ☐ Latest 212-89 Exam Preparation
- Free PDF EC-COUNCIL - 212-89 - EC Council Certified Incident Handler (ECIH v3) –The Best Valid Exam Testking ☐  
☐ Open [ [www.prep4pass.com](http://www.prep4pass.com) ] and search for ☀ 212-89 ☐☀☐ to download exam materials for free ☐ Latest 212-89 Exam Bootcamp
  - Newly Released EC-COUNCIL 212-89 Dumps in Three Formats [2025] ☐ Search on ➡ [www.pdfvce.com](http://www.pdfvce.com) ☐ for 「 212-89 」 to obtain exam materials for free download ☐ Books 212-89 PDF
  - Popular 212-89 Exams ☐ Latest 212-89 Exam Bootcamp ☐ 212-89 Examcollection ☐ Search for ✓ 212-89 ☐✓☐ and download it for free on 「 [www.prep4pass.com](http://www.prep4pass.com) 」 website ☐ 212-89 Pdf Dumps
  - The Best Accurate Valid 212-89 Exam Testking - Easy and Guaranteed 212-89 Exam Success ☐ Search for [ 212-89 ] on ☀ [www.pdfvce.com](http://www.pdfvce.com) ☐☀☐ immediately to obtain a free download ☐ New 212-89 Test Tutorial
  - Latest 212-89 Reliable Torrent - 212-89 Actual Pdf - 212-89 Exam Questions ☐ Search for ➡ 212-89 ☐ and easily obtain a free download on 「 [www.real4dumps.com](http://www.real4dumps.com) 」 ☐ Pdf Demo 212-89 Download
  - 212-89 New Brindumps Sheet ☐ 212-89 Test Dumps ☐ 212-89 Clearer Explanation ☐ Copy URL ➡ [www.pdfvce.com](http://www.pdfvce.com) ☐ open and search for ⇒ 212-89 ⇐ to download for free ➡ 212-89 Clearer Explanation
  - Latest 212-89 Exam Bootcamp ☐ Latest 212-89 Exam Preparation ☐ Test 212-89 Free ☐ Copy URL ( [www.free4dump.com](http://www.free4dump.com) ) open and search for ➡ 212-89 ☐ to download for free ☐ 212-89 Test Guide
  - [kelastokuteiginou.com](http://kelastokuteiginou.com), [myportal.utt.edu.tt](http://myportal.utt.edu.tt), [myportal.utt.edu.tt](http://myportal.utt.edu.tt), [myportal.utt.edu.tt](http://myportal.utt.edu.tt), [myportal.utt.edu.tt](http://myportal.utt.edu.tt), [myportal.utt.edu.tt](http://myportal.utt.edu.tt), [myportal.utt.edu.tt](http://myportal.utt.edu.tt), [myportal.utt.edu.tt](http://myportal.utt.edu.tt), [myportal.utt.edu.tt](http://myportal.utt.edu.tt), [myportal.utt.edu.tt](http://myportal.utt.edu.tt), [www.holisticwisdom.com.au](http://www.holisticwisdom.com.au), [netflowbangladesh.com](http://netflowbangladesh.com), [adrcentre.org](http://adrcentre.org), [elearning.eauquardho.edu.so](http://elearning.eauquardho.edu.so), [888.8337.net](http://888.8337.net), [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [eab.com.bd](http://eab.com.bd), Disposable vapes

What's more, part of that PDF4Test 212-89 dumps now are free: <https://drive.google.com/open?id=1APJ6CEZ2pZkZD42BQAGm0uiMkQPw7cl>