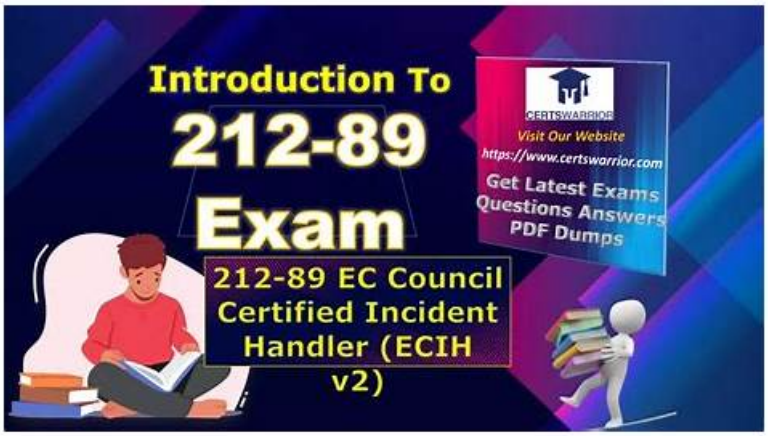
Preparing EC-COUNCIL 212-89 Exam is Easy with Our High-quality 212-89 Actual Tests: EC Council Certified Incident Handler (ECIH v3)



P.S. Free 2026 EC-COUNCIL 212-89 dumps are available on Google Drive shared by ValidBraindumps: https://drive.google.com/open?id=1bFKqcdKNXocpVuePhI1ZL53SpG_o6af7

You can choose the most suitable and convenient one for you. The web-based 212-89 practice exam is compatible with all operating systems. It is a browser-based EC-COUNCIL 212-89 Practice Exam that works on all major browsers. This means that you won't have to worry about installing any complicated software or plug-ins.

The EC-Council Certified Incident Handler (ECIH) certification exam is designed for individuals who work in the field of incident handling and response. The ECIH certification is a vendor-neutral certification that validates an individual's skills in managing and responding to various types of security incidents. The ECIH certification exam is intended for security professionals who want to validate their skills and knowledge in incident handling and response.

To become certified in ECIH v2, candidates must pass a rigorous certification exam that tests their knowledge, skills, and abilities in the areas of incident handling and response. 212-89 Exam consists of 100 multiple-choice questions, and candidates have 3 hours to complete the exam. 212-89 exam is designed to test the candidate's knowledge of incident handling and response techniques, as well as their ability to analyze and respond to security incidents.

>> 212-89 Actual Tests <<

EC Council Certified Incident Handler (ECIH v3) test for engine, 212-89 VCE test engine

If you buy online classes, you will need to sit in front of your computer on time at the required time; if you participate in offline counseling, you may need to take an hour or two of a bus to attend class. So even if you are a newcomer, you don't need to worry that you can't understand the contents. Industry experts hired by 212-89 Exam Questions also explain all of the difficult professional vocabulary through examples, forms, etc. You can completely study alone without the help of others.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q273-Q278):

NEW QUESTION # 273
The insider risk matrix consists of technical literacy and business process knowledge vectors. Considering the matrix, one can conclude that:

- A. If the insider's technical literacy is high and process knowledge is low, the risk posed by the threat will be high.
- B. If the insider's technical literacy and process knowledge are high, the risk posed by the threat will be insignificant.

- C. If the insider's technical literacy is low and process knowledge is high, the risk posed by the threat will be insignificant.
- D. If the insider's technical literacy and process knowledge are high, the risk posed by the threat will be high.

Answer: D

NEW QUESTION # 274
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. Immediately notify law enforcement and regulatory bodies.
- B. Conduct a network-wide vulnerability scan.
- C. Isolate the affected network segment and manually inspect each endpoint.
- D. Deploy an endpoint detection and response (EDR) solution to identify and investigate suspicious activities.

Answer: D

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 # 275
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 5
- B. Principle 3
- C. Principle 7
- D. Principle 2

Answer: A

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 # 276
The steps followed to recover computer systems after an incident are:

- A. System monitoring, validation, operation and restoration
- B. System restoration, validation, operation and monitoring
- C. System restoration, operation, validation, and monitoring

- D. System validation, restoration, operation and monitoring

Answer: B

NEW QUESTION # 277
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. 2 -> 1 -> 3 -> 6 -> 4 -> 5
- B. 5-> 2-> l-> 3-> 4-> 6
- C. 3 .> 2 -> 1 -> 4-> 6-> 5
- D. 2->3->l ->4->6->5

Answer: A

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 # 278
.....

obtain { 212-89 } for free download through ⇛ www.pdfvce.com ⇚ ♣Official 212-89 Practice Test

- 212-89 EC Council Certified Incident Handler (ECIH v3) Web-Based Practice Exam The page for free download of 【 212-89 】 on 「 www.vce4dumps.com 」 will open immediately Valid Dumps 212-89 Book
- myportal.utt.edu.tt, www.stes.tyc.edu.tw, bbs.t-firefly.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free 2026 EC-COUNCIL 212-89 dumps are available on Google Drive shared by ValidBraindumps: https://drive.google.com/open?id=1bFKqcdKNXocpVuePhI1ZL53SpG_o6af7