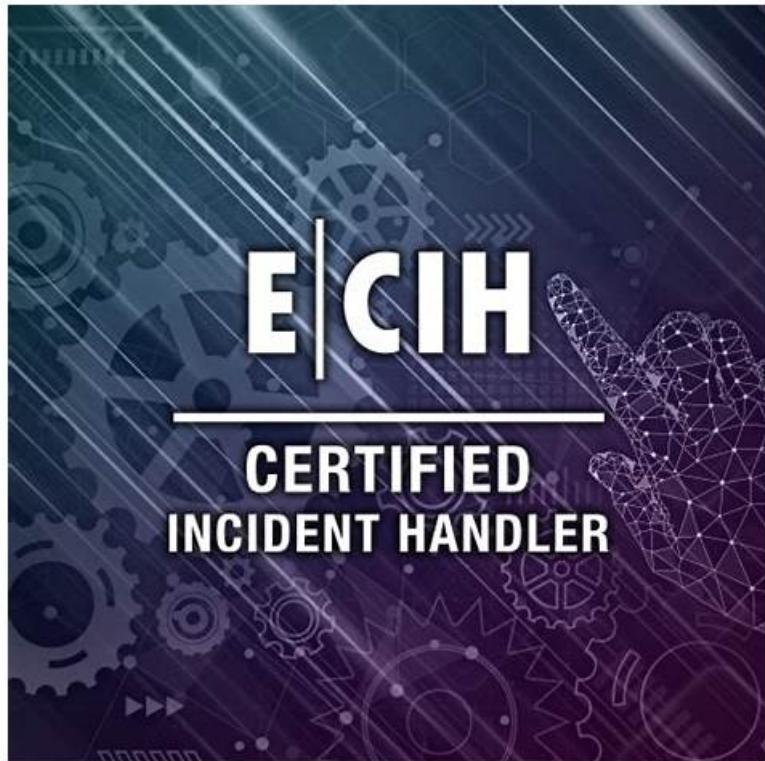


EC-COUNCIL - 212-89 - Marvelous EC Council Certified Incident Handler (ECIH v3) Valid Test Registration



What's more, part of that ValidDumps 212-89 dumps now are free: <https://drive.google.com/open?id=15Gaqh88N8PtQ0LuXzvdqvLXM7tD2D6xh>

Our PDF version, online test engine and windows software of the EC Council Certified Incident Handler (ECIH v3) study materials have no restrictions to your usage. You can freely download our PDF version and print it on papers. Also, you can share our 212-89 study materials with other classmates. The online test engine of the study materials can run on all windows system, which means you can begin your practice without downloading the 212-89 Study Materials as long as there have a computer. Also, our windows software support downloading for many times. What is more, you can install our 212-89 study materials on many computers. All of them can be operated normally. The three versions of 212-89 study materials are excellent. Just choose them as your good learning helpers.

EC-COUNCIL 212-89: EC Council Certified Incident Handler (ECIH v2) exam is a valuable certification for IT professionals who want to advance their careers in the information security field. EC Council Certified Incident Handler (ECIH v3) certification validates the candidate's ability to handle security incidents effectively, and the course content includes practical scenarios that simulate real-world security incidents. Candidates who pass the exam will have a deeper understanding of incident handling procedures and be able to apply them effectively in their organizations.

The EC-Council 212-89, also known as the EC Council Certified Incident Handler (ECIH v2) exam, is a certification program designed to validate an individual's knowledge and skills in identifying, responding, and resolving computer security incidents. EC Council Certified Incident Handler (ECIH v3) certification exam is intended for IT professionals who are responsible for managing, detecting, preventing, and responding to security incidents in organizations.

>> 212-89 Valid Test Registration <<

Pass Guaranteed Quiz 212-89 - EC Council Certified Incident Handler (ECIH v3) Useful Valid Test Registration

EC-COUNCIL 212-89 practice test software contains many EC-COUNCIL 212-89 practice exam designs just like the real EC Council Certified Incident Handler (ECIH v3) (212-89) exam. These 212-89 practice exams contain all the 212-89 questions that

clearly and completely elaborate on the difficulties and hurdles you will face in the final 212-89 Exam. We update our EC-COUNCIL 212-89 exam questions bank regularly to match the changes and improve the quality of 212-89 questions so you can get a better experience.

EC-COUNCIL 212-89 certification exam covers a range of topics related to incident handling, including incident response process and procedures, digital forensics, network security essentials, and vulnerability management. 212-89 Exam consists of 100 multiple-choice questions, and candidates are given two hours to complete it. 212-89 exam is computer-based and can be taken at one of EC-COUNCIL's authorized testing centers.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q222-Q227):

NEW QUESTION # 222

Attackers or insiders create a backdoor into a trusted network by installing an unsecured access point inside a firewall. They then use any software or hardware access point to perform an attack.

Which of the following is this type of attack?

- A. Rogue access point attack
- B. Malware attack
- C. Password-based attack
- D. Email infection

Answer: A

NEW QUESTION # 223

If a hacker cannot find any other way to attack an organization, they can influence an employee or a disgruntled staff member. What type of threat is this?

- A. Insider attack
- B. Identity theft
- C. Footprinting
- D. Phishing attack

Answer: A

Explanation:

If a hacker influences an employee or a disgruntled staff member to gain access to an organization's resources or sensitive information, this is classified as an insider attack. Insider attacks are perpetrated by individuals within the organization, such as employees, contractors, or business associates, who have inside information concerning the organization's security practices, data, and computer systems. The threat from insiders can be intentional, as in the case of a disgruntled employee seeking to harm the organization, or unintentional, where an employee is manipulated or coerced by external parties without realizing the implications of their actions.

Phishing attacks, footprinting, and identity theft represent different types of cybersecurity threats where the attacker's method or objective differs from that of insider attacks. References: The ECIH v3 certification program addresses various types of threats, including insider threats, emphasizing the importance of recognizing and mitigating risks posed by individuals within the organization.

NEW QUESTION # 224

Which of the following is not a countermeasure to eradicate inappropriate usage incidents?

- A. Registering user activity logs and keep monitoring them regularly
- B. Installing firewall and IDS/IPS to block services that violate the organization's policy
- C. Always storing the sensitive data in far located servers and restricting its access
- D. Avoiding VPN and other secure network channels

Answer: D

NEW QUESTION # 225

Which of the following risk mitigation strategies involves execution of controls to reduce the risk factor and brings it to an acceptable level or accepts the potential risk and continues operating the IT system?

- A. Risk transference
- **B. Risk assumption**
- C. Risk avoidance
- D. Risk planning

Answer: B

Explanation:

Risk assumption involves accepting the potential risk and continuing to operate the IT system while implementing controls to reduce the risk to an acceptable level. This strategy acknowledges that some level of risk is inevitable and focuses on managing it through mitigation measures rather than eliminating it entirely.

Risk avoidance would entail taking actions to avoid the risk entirely, risk planning involves preparing for potential risks, and risk transference shifts the risk to another party, typically through insurance or outsourcing.

Risk assumption is a pragmatic approach that balances the need for operational continuity with the imperative of risk management. References: The ECIH v3 certification program covers various risk mitigation strategies, emphasizing the selection of the appropriate approach based on the organization's risk tolerance and the specific context of the threat.

NEW QUESTION # 226

Which of the following is an Inappropriate usage incident?

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

Answer: C

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 # 227

.....

Valid Braindumps 212-89 Free: <https://www.validdumps.top/212-89-exam-torrent.html>

- Free PDF Quiz Updated 212-89 - EC Council Certified Incident Handler (ECIH v3) Valid Test Registration Simply search for { 212-89 } for free download on “ www.vce4dumps.com ” ↴ New 212-89 Test Braindumps
- Dumps 212-89 Questions 212-89 Well Prep Valid 212-89 Learning Materials Copy URL www.pdfvce.com ↴ open and search for “ 212-89 ” to download for free 212-89 Valid Test Fee
- 2026 100% Free 212-89 –The Best 100% Free Valid Test Registration | Valid Braindumps 212-89 Free Search for ➔ 212-89 on (www.prepawayete.com) immediately to obtain a free download 212-89 Latest Test Report
- Dumps 212-89 Questions Dumps 212-89 Questions 212-89 Test Vce Simply search for ➔ 212-89 for free download on www.pdfvce.com 212-89 Popular Exams
- Last 212-89 Exam Dumps: EC Council Certified Incident Handler (ECIH v3) help you pass 212-89 exam surely - www.troytecdumps.com Search for 212-89 and download it for free on www.troytecdumps.com ↴ website 212-89 New Test Materials
- New 212-89 Exam Book 212-89 New Test Materials New 212-89 Test Braindumps The page for free download of 212-89 on www.pdfvce.com ↴ will open immediately 212-89 Latest Test Report

BONUS!!! Download part of ValidDumps 212-89 dumps for free: <https://drive.google.com/open?id=15Gaqh88N8PtQ0LuXzvdqvLXM7tD2D6xh>