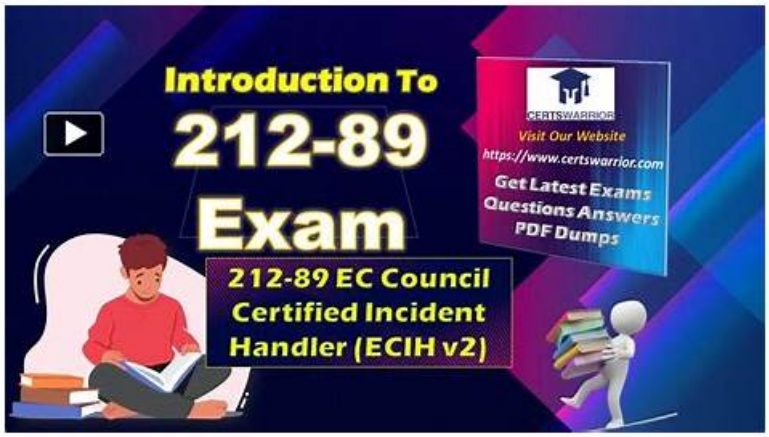
# 212-89 Latest Exam Format - 212-89 Exam Passing Score




BONUS!!! Download part of Exams4Collection 212-89 dumps for free: https://drive.google.com/open?id=1tpftVf3OtMkHRbjajmSTO0yGEYXQmJFm

Exams4Collection EC-COUNCIL 212-89 exam preparation material is designed to help you pass the EC-COUNCIL 212-89 exam on your first attempt. The formats mentioned above can be used right away after buying the product. So what are waiting for, get our EC Council Certified Incident Handler (ECIH v3) (212-89) study material today and start your constructive progress towards your goals. The rest is assured by us when you give it your all.

Since the 212-89 study quiz is designed by our professionals who had been studying the exam all the time according to the changes of questions and answers. Our 212-89 simulating exam is definitely making your review more durable. To add up your interests and simplify some difficult points, our experts try their best to simplify our 212-89 Study Material and help you understand the learning guide better.

**>> 212-89 Latest Exam Format <<**

## 212-89 Exam Passing Score & 212-89 Latest Braindumps Free

To save resources of our customers, we offer real EC Council Certified Incident Handler (ECIH v3) (212-89) exam questions that are enough to master for 212-89 certification exam. Our EC-COUNCIL 212-89 Exam Dumps are designed by experienced industry professionals and are regularly updated to reflect the latest changes in the Building EC Council Certified Incident Handler (ECIH v3) (212-89) exam content.

## Exam Topic Areas

**All in all, the ECIH 212-89 Exam will cover the following topic areas:**

- Application-Level Incidents;
- Process Handling;
- Malware Incidents;
- Forensic Readiness and First Response;
- Insider Threats;
- Incidents Occurred in a Cloud Environment.
- Network & Mobile Incidents;
- Incident Response and Handling;

## EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q119-Q124):

**NEW QUESTION # 119**
A national research agency was recently subjected to a comprehensive cybersecurity compliance audit.
During the audit, reviewers evaluated how the agency's incident response unit manages harmful code samples during investigations.

The assessment revealed that team members often interacted with dangerous file payloads directly on enterprise-connected systems used for general operations. Furthermore, no precautionary renaming was applied to prevent accidental triggering, and sensitive materials were placed in areas accessible by non-specialized personnel. The auditors flagged these practices as severely noncompliant with safe sample processing protocols and recommended urgent changes to prevent operational fallout or accidental outbreaks.
Which best practice for secure handling of malicious code was most clearly disregarded in this case?

- A. Storing malware samples with non-executable file extensions in isolated environments.
- B. Encrypting all malware sample files using symmetric encryption.
- C. Create vulnerability documentation for each malware sample to support threat profiling and archival.
- D. Tagging malware sample files with platform-specific behavior indicators for improved categorization.

**Answer: A**

Explanation:
Comprehensive and Detailed Explanation (ECIH-aligned):
This scenario highlights violations of forensic readiness and safe malware handling, which are explicitly covered in the ECIH First Response and Malware Analysis modules. ECIH stresses that malware samples must never be handled on production or enterprise-connected systems, as this creates a high risk of accidental execution, lateral infection, and organizational impact.
Option A is correct because ECIH mandates that malicious code samples be stored in isolated, non- networked environments and renamed with non-executable extensions (for example, .malware, .bin, or .txt) to prevent accidental execution. This practice ensures operational safety and preserves forensic integrity.
Option B improves confidentiality but does not prevent accidental execution. Option C supports documentation but does not mitigate execution risk. Option D aids classification but does not address safe handling.
The described behavior-handling live malware on enterprise systems without isolation or renaming- directly contradicts ECIH best practices. Proper sample isolation, renaming, and access restriction are mandatory controls to prevent secondary incidents during investigations, making Option A the correct answer.

**NEW QUESTION # 120**
At a major healthcare provider, staff received phishing emails impersonating HR. Reporting via email failed due to mail system issues. The IR team introduced VOIP and SMS-based reporting mechanisms. Which preparatory step was implemented?

- A. Creating backup archives
- B. Training on phishing indicators
- C. Email content filtering
- D. Establishing out-of-band communication

**Answer: D**

Explanation:
This scenario highlights a preparation phase improvement. ECIH strongly emphasizes the importance of out- of-band communication during incidents, especially when primary systems are compromised.
Option D is correct because VOIP and SMS reporting channels allow incident reporting even when email systems are unavailable or under attack. ECIH identifies out-of-band communication as critical for maintaining coordination and timely escalation during incidents.
Options A-C do not address the reporting failure described.
Establishing alternate communication channels strengthens incident readiness and response resilience, aligning directly with ECIH best practices.

**NEW QUESTION # 121**
During routine monitoring, a cloud-based application hosting provider detects an anomaly suggesting an ongoing DDoS attack targeting one of its hosted applications. The provider's incident response team must quickly mitigate the attack while ensuring minimal service disruption. Which of the following strategies should they prioritize?

- A. Implement rate limiting and challenge-response tests to differentiate between legitimate and malicious traffic.
- B. Temporarily take the affected application offline to stop the attack.
- C. Immediately scale up application resources to absorb the attack impact.
- D. Enable geo-restriction to block incoming traffic from regions not serviced by the application.

**Answer: A**

Explanation:
The ECIH Network Security Incident Handling module emphasizes maintaining availability while mitigating denial-of-service attacks. The objective is not simply to stop traffic, but to distinguish malicious traffic from legitimate user requests.
Option D is correct because rate limiting and challenge-response mechanisms (such as CAPTCHA or SYN cookies) allow legitimate traffic to continue while throttling or blocking malicious requests. This approach minimizes service disruption while effectively containing the attack.
Option A may increase costs and still fail against large-scale DDoS attacks. Option B can unintentionally block legitimate users. Option C contradicts ECIH guidance by unnecessarily impacting availability.
ECIH stresses proportional and intelligent mitigation strategies that preserve business continuity. Therefore, implementing rate limiting and challenge-response mechanisms is the preferred strategy.

**NEW QUESTION # 122**
Which of the following is a standard framework that provides recommendations for implementing information security controls for organizations that initiate, implement, or maintain information security management systems (ISMSs)?

- A. PCI DSS
- B. RFC 219G
- C. ISO/IEC 27002
- D. ISO/IEC 27035

**Answer: C**

**NEW QUESTION # 123**
Finn is working in the eradication phase, wherein he is eliminating the root cause of an incident that occurred in the Windows operating system installed in a system. He ran a tool that can detect missing security patches and install the latest patches on the system and networks. Which of the following tools did he use to detect the missing security patches?

- A. Office360 Advanced Throat Protection
- B. Microsoft Cloud App Security
- C. Microsoft Baseline Security Analyzer
- D. Microsoft Advanced Threat Analytics

**Answer: C**

**NEW QUESTION # 124**
.....

- Latest 212-89 Exam Vce □ Reliable 212-89 Exam Tutorial □ Latest 212-89 Questions □ The page for free download of ➠ 212-89 □ on [ www.examcollectionpass.com ] will open immediately □Latest 212-89 Questions
- Reliable 212-89 Exam Tutorial □ 212-89 Reliable Dumps Book □ 212-89 Vce Format □ Download ✔ 212-89 □✔□ for free by simply entering ➡ www.pdfvce.com □□□ website □Practice 212-89 Test Online
- Reliable 212-89 Exam Tutorial □ Reliable 212-89 Test Labs □ 212-89 Test Guide Online □ Search for ⇛ 212-89 ⇚ and download exam materials for free through 《 www.troytecdumps.com 》 □Latest 212-89 Questions
- Here's the Proven and Quick Way to Pass EC-COUNCIL 212-89 Exam □ Easily obtain { 212-89 } for free download through 【 www.pdfvce.com 】 □Valid 212-89 Test Discount
- 2026 EC-COUNCIL Accurate 212-89: EC Council Certified Incident Handler (ECIH v3) Latest Exam Format □ Search for ➠ 212-89 □ and download it for free on 「 www.verifieddumps.com 」 website □Test 212-89 Collection Pdf
- zoyasgrr195954.wikiexcerpt.com, bookmarkbooth.com, lawsonzkyr449626.wannawiki.com, jadadcyp677429.thenerdsblog.com, kianafgsb527089.gigswiki.com, www.stes.tyc.edu.tw, 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, charliephsh579336.bloggerswise.com, madbookmarks.com, Disposable vapes

What's more, part of that Exams4Collection 212-89 dumps now are free: https://drive.google.com/open?id=1tpftVf3OtMkHRbjajmSTO0yGEYXQmJFm