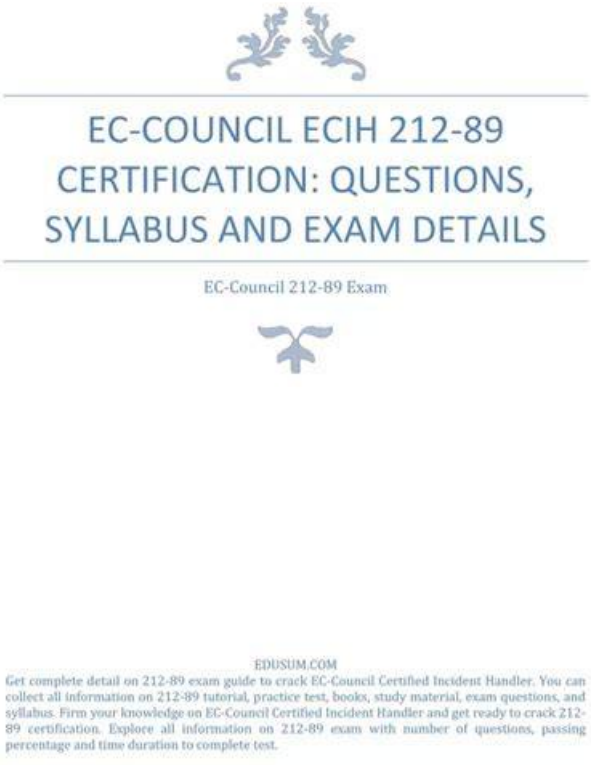
100% Pass 2026 Authoritative EC-COUNCIL 212-89 Certificate Exam



What's more, part of that Prep4King 212-89 dumps now are free: https://drive.google.com/open?id=1Qc35sc5UV4KnxsnJi6VZf2CJbNOLX9ct

We continually improve the versions of our 212-89 exam guide so as to make them suit all learners with different learning levels and conditions. The clients can use the APP/Online test engine of our 212-89 exam guide in any electronic equipment such as the cellphones, laptops and tablet computers. Our after-sale service is very considerate and the clients can consult our online customer service about the price and functions of our 212-89 Quiz materials. So our 212-89 certification files are approximate to be perfect and will be a big pleasant surprise after the clients use them.

EC-COUNCIL 212-89 Exam Syllabus Topics:

Section	Weight	Objectives
Topic 1: Handling and Responding to Endpoint Security Incidents	13%	- Endpoint threats and vulnerabilities • 1. Endpoint attack vectors • 2. Unpatched systems, misconfigurations - Endpoint incident response • 1. Investigating compromised endpoints • 2. Remediation and hardening

Topic 2: Incident Handling Process	15%	- Preparation phase • 1. Developing incident response policies • 2. Building incident response teams - Containment, eradication, and recovery • 1. Restoring systems and services • 2. Eradicating threats and vulnerabilities • 3. Strategies for containment - Detection and analysis phase • 1. Classifying and prioritizing incidents • 2. Identifying security incidents - Lessons learned and improvement • 1. Updating policies and procedures • 2. Conducting post-incident reviews
Topic 3: Post-Incident Activities and Reporting	7%	- Incident documentation and reporting • 1. Creating incident reports • 2. Communicating with stakeholders - Response and mitigation strategies • 1. Blocking malicious traffic • 2. Securing network infrastructure
Topic 4: Handling and Responding to Network Security Incidents	15%	- Network attacks and threats • 1. Network intrusion techniques • 2. DDoS, man-in-the-middle, SQL injection - Network incident detection and analysis • 1. Monitoring network traffic • 2. Using IDS/IPS tools - Legal and ethical aspects • 1. Privacy and data protection • 2. Compliance requirements
Topic 5: Introduction to Incident Handling and Response	12%	- Fundamentals of incident handling and response • 1. Incident response lifecycle • 2. Key concepts and terminology
Topic 6: Handling and Responding to Cloud Security Incidents	10%	- Cloud incident response process • 1. Detecting and analyzing cloud incidents • 2. Responding in multi-tenant environments - Cloud computing concepts and risks • 1. Cloud-specific threats • 2. Cloud service models and deployment models

Topic 7: Handling and Responding to Malware Incidents	18%	- Malware analysis techniques • 1. Identifying malware behavior • 2. Static and dynamic analysis - Malware incident response procedures • 1. Isolating infected systems • 2. Removing malware and recovering - Types of malware and attack vectors • 1. Viruses, worms, trojans, ransomware • 2. Social engineering and phishing

>> 212-89 Certificate Exam <<

Well-known 212-89 Practice Materials Offer You Perfect Exam Braindumps-Prep4King

Prep4King 212-89 exam braindumps is valid and cost-effective, which is the right resource you are looking for. What you get from the 212-89 practice torrent is not only just passing with high scores, but also enlarging your perspective and enriching your future. From the 212-89 free demo, you will have an overview about the complete exam dumps. The comprehensive questions together with correct answers are the guarantee for 100% pass.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q332-Q337):

NEW QUESTION # 332
Smith employs various malware detection techniques to thoroughly examine the network and its systems for suspicious and malicious malware files. Among all techniques, which one involves analyzing the memory dumps or binary codes for the traces of malware?

- A. Dynamic analysis
- B. Live system
- C. Static analysis
- D. Intrusion analysis

Answer: C

Explanation:
Static analysis involves examining the malware's memory dumps or binary codes without executing the code.
This technique is used to find traces of malware by analyzing the code to understand its purpose, functionality, and potential impact.
Static analysis allows for the identification of malicious signatures, strings, or other indicators of compromise within the malware's code. This method is contrasted with dynamic analysis, which studies the malware's behavior during execution, live system analysis, which examines running systems, and intrusion analysis, which focuses on detecting and analyzing breaches.References:The ECIH v3 certification program includes malware analysis techniques, highlighting static analysis as a key method for investigating malware without the risk of executing it on a live system.

NEW QUESTION # 333
A logistics company relying heavily on cloud-based inventory management discovered unauthorized activity initiated by a third-party contractor. The investigation revealed that the contractor's login was reused across multiple departments and lacked any tracking mechanism or role-specific restrictions to limit its scope. What cloud security best practice should be implemented to prevent such violations?

- A. Implementation of Secure Sockets Layer (SSL) encryption on internal dashboards.
- B. Routine vulnerability scans on mobile apps used by delivery teams.
- C. Enforcement of strict user access control and credential isolation.
- D. Use of anonymized data during inventory analytics.

Answer: C

Explanation:
Strict user access control and credential isolation ensure each contractor has a unique, traceable account with permissions limited to their assigned role. This prevents shared login abuse, improves accountability, and limits unauthorized access across departments.

NEW QUESTION # 334
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. Footprinting
- B. Phishing attack
- C. Identity theft
- D. Insider attack

Answer: D

NEW QUESTION # 335
Lena, a SOC analyst, observes a pattern of unusual login attempts originating from multiple foreign IP addresses tied to shared drive links circulating within the organization. These links were embedded in emails appearing to come from the HR department and marked with urgent subject lines. Upon deeper inspection, Lena finds multiple similar messages still pending in the mail server's delivery queue. To prevent widespread exposure, she takes immediate action to eliminate these messages before they reach employees' inboxes.
Which incident response action best describes Lena's action?

- A. Flagging login anomalies for correlation in the SIEM
- B. Isolating compromised mailboxes from the email relay
- C. Preemptively purging queued phishing emails from the server
- D. Initiating forensic triage on suspicious attachments

Answer: C

Explanation:
This scenario demonstrates a preventive containment action during an email security incident. The ECIH Email Security Incident Handling module emphasizes that once phishing is identified, responders should immediately prevent further delivery to reduce organizational exposure.
Option A is correct because Lena removes malicious emails from the mail server's delivery queue before users receive them. This action directly reduces risk by preventing additional users from clicking malicious links or submitting credentials. ECIH identifies email purging as a critical containment technique during active phishing campaigns.
Option B is an investigative action, not containment. Option C applies after delivery and compromise. Option D addresses already compromised accounts rather than preventing exposure.
By stopping malicious emails before delivery, Lena aligns with ECIH best practices for rapid containment of email-based threats.

NEW QUESTION # 336
Which of the following is a technique used by attackers to make a message difficult to understand through the use of ambiguous language?

- A. Spoofing
- B. Steganography
- C. Obfuscation
- D. Encryption

Answer: C

Explanation:
Obfuscation is a technique used to make data or code difficult to understand. It is often employed by attackers to conceal the true intent of their code or communications, making it harder for security professionals, automated tools, and others to analyze or detect malicious activity. Obfuscation can involve the use of ambiguous or misleading language, as well as more technical methods such as

encoding, encryption, or the use of nonsensical variable names in source code to hide its true functionality.
References:The ECIH v3 program discusses various techniques attackers use to evade detection, including obfuscation, highlighting how it complicates the analysis and understanding of malicious payloads.

NEW QUESTION # 337
.....

In recruiting employees as IT engineers many companies look for evidence of all-round ability especially constantly studying ability more their education background. 212-89 dumps torrent can help you fight for EC-COUNCIL certification and achieve your dream in the shortest time. If you want to stand out from the crowd, purchasing a valid 212-89 Dumps Torrent will be a shortcut to success. It will be useful for you to avoid detours and save your money & time.