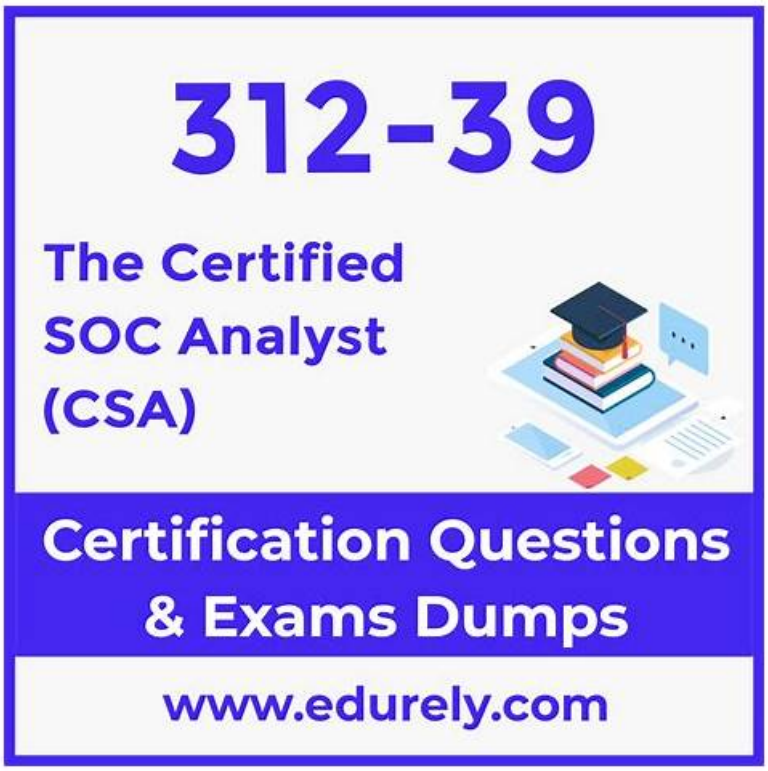
312-39 Valid Exam Cost & Exam 312-39 Pass4sure



P.S. Free & New 312-39 dumps are available on Google Drive shared by Exam4PDF: https://drive.google.com/open?id=1VkWLg0YaiaALac6cIYm7QTBYCJTaqISn

Exam4PDF IT experts specialize in training way which is the latest short-term effective. This training method is very helpful to you and you can achieve the expected result. In particular, it brings convenience to these candidates both working and studying. To the best of our knowledge the information contained in this publication is accurate. Exam4PDF EC-COUNCIL 312-39 Test Questions and test answers have an advantage over other products with the accuracy of 100%. You may be worried that our 312-39 practice test is old version. Don't worry, Our Exam4PDF EC-COUNCIL 312-39 exam dumps is the latest. Free update is for one year.

The EC-Council Certified SOC Analyst (CSA) certification is a popular certification program designed to equip professionals with the necessary skills to protect organizations against cyber threats. Certified SOC Analyst (CSA) certification is designed for professionals who work in Security Operations Centers (SOC) and are responsible for detecting, analyzing, and responding to cybersecurity incidents. Certified SOC Analyst (CSA) certification validates the expertise of SOC analysts and equips them with the necessary skills to perform their duties effectively.

To prepare for the exam, candidates can take advantage of a range of resources provided by EC-COUNCIL, including training courses, study guides, and practice exams. These resources are designed to help candidates develop the knowledge and skills they need to succeed on the exam and in their careers as SOC analysts.

>> 312-39 Valid Exam Cost <<

Exam 312-39 Pass4sure - Valid 312-39 Test Papers

312-39 certifications are thought to be the best way to get good jobs in the high-demanding market. There is a large range of 312-39 certifications that can help you improve your professional worth and make your dreams come true. Our 312-39 Certification Practice materials provide you with a wonderful opportunity to get your dream certification with confidence and ensure your success by your first attempt.

EC-COUNCIL 312-39 Certified SOC Analyst (CSA) certification exam is a crucial step for IT and security professionals who aim to build a career in security operations centers (SOC). Certified SOC Analyst (CSA) certification is designed to validate the candidate's knowledge and skills related to SOC operations, including threat detection, response, and mitigation. 312-39 Exam focuses on a wide range of topics, including security operations, incident management, threat intelligence, and risk management.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q129-Q134):

NEW QUESTION # 129
Which of the following contains the performance measures, and proper project and time management details?

- A. Incident Response Procedures
- B. Incident Response Policy
- C. Incident Response Process
- D. Incident Response Tactics

Answer: B

Explanation:


NEW QUESTION # 130
Following a high-priority security incident, you, as an Incident Responder at a Cyber Incident Response firm, initiate an internal investigation after reports confirm a serious data breach in which sensitive customer data, including payment details and personal information, was stolen from a critical web server. You begin analyzing the server logs to reconstruct the attack timeline and identify how the attacker gained access.
During your investigation, you discover suspicious activity in the logs, including repeated requests attempting to access files and directories outside of the web server's root directory. Some of these requests appear to be manipulating URL paths to navigate into restricted system files-a behavior that is often associated with web- based exploits. You suspect that a vulnerability in the web server was exploited to bypass security restrictions and access unauthorized directories, potentially exposing sensitive configurations and credentials. However, you still need to confirm the exact technique used. Which type of web application attack might have caused this incident?

- A. Directory Traversal
- B. Session Attacks: Cookie Poisoning
- C. Cross-Site Scripting (XSS) Attacks
- D. SQL Injection Attack

Answer: A

Explanation:
Directory Traversal is the technique most directly aligned with "manipulating URL paths to access files and directories outside the web root." Attackers abuse path sequences (for example, patterns like "../") or encoded variants to move upward in a directory structure and reach restricted locations such as configuration files, credentials, or system files. In SOC investigations, repeated attempts to request "outside-root" paths in web logs (often with URL encoding, double encoding, or mixed separators) is a classic indicator of traversal probing and exploitation. This differs from SQL injection, which targets database queries and typically shows payloads manipulating SQL syntax (quotes, UNION, tautologies, time delays) rather than filesystem path navigation. XSS focuses on injecting scripts into web pages to run in a victim's browser, so the log artifacts are more about injected JavaScript/HTML

payloads and reflected/stored contexts. Cookie poisoning is a session attack involving tampering with session tokens or cookie values, which shows up as abnormal cookie parameters rather than path traversal requests. Given the explicit evidence of path manipulation to reach unauthorized directories, Directory Traversal is the best match and should drive mitigations such as strict input validation, canonical path checks, least-privilege file permissions, and WAF rules.

NEW QUESTION # 131
Which of the following data source can be used to detect the traffic associated with Bad Bot User-Agents?

- A. Switch Logs
- B. Router Logs
- C. Windows Event Log
- D. Web Server Logs

Answer: D

Explanation:
Bad bots are automated software that perform tasks over the internet, which can sometimes be malicious, like scraping data, spamming, or carrying out credential stuffing attacks. To detect the traffic associated with Bad Bot User-Agents, web server logs are the most effective data source. These logs record all the requests made to the web server, including the User-Agent string that identifies the type of client making the request. By analyzing these logs, SOC analysts can identify patterns and behaviors indicative of bad bots, such as high request rates, unusual access patterns, or known malicious User-Agent strings.
References: The EC-Council's Certified SOC Analyst (CSA) program covers the fundamentals of SOC operations, including log management and correlation, which is essential for detecting bad bots. The CSA certification program provides the knowledge required to use various tools and techniques for monitoring and analyzing web server logs for potential threats. For more detailed information, refer to the official EC-Council SOC Analyst study guides and training resources1234.

NEW QUESTION # 132
In which of the following incident handling and response stages, the root cause of the incident must be found from the forensic results?

- A. Eradication
- B. Evidence Handling
- C. SystemsRecovery
- D. Evidence Gathering

Answer: A

Explanation:
The eradication stage is where the root cause of the incident is determined from the forensic results. This stage involves not only removing the threat from the affected systems but also identifying and fixing the vulnerabilities that were exploited. It's crucial to understand how the incident occurred to prevent future occurrences. After the containment stage, where the immediate threat is isolated, eradication ensures that the threat is completely removed and that the root cause is addressed.
References: The EC-Council's Certified Incident Handler (E|CIH) program outlines the stages of incident handling and response, which include preparation, identification, containment, eradication, recovery, and lessons learned. Theeradication stage specifically deals with eliminating the threat and addressing the root cause based on forensic analysis. This information is covered in the E|CIH program and can be found in the official EC-Council learning resources1.
Reference: https://www.eccouncil.org/wp-content/uploads/2019/02/ECIH-V2-Brochure.pdf

NEW QUESTION # 133
Which of the following attack can be eradicated by converting all non-alphanumeric characters to HTML character entities before displaying the user input in search engines and forums?

- A. WebServices Attacks
- B. Broken Access Control Attacks
- C. XSS Attacks
- D. Session Management Attacks

Answer: C

Explanation:
Converting all non-alphanumeric characters to HTML character entities is a common defense against Cross- Site Scripting (XSS) attacks. Here's how it works:
* User Input Sanitization: When user input is received, the system converts characters like <, >, &, ', and " into their corresponding HTML entities (e.g., <, >, &, ', and ").
* Preventing Script Execution: By converting these characters, the system prevents potentially malicious scripts from being executed in the browser of anyone viewing the content.
* Maintaining Data Integrity: This process allows user-generated content to be displayed without altering the intended message while ensuring the content cannot harm other users or the system.
References:
EC-Council's Certified SOC Analyst (C|SA) course material covers various cybersecurity threats, including XSS attacks, and the methods used to mitigate them.
The study guides and resources provided by EC-Council for the SOC Analyst certification include detailed explanations of XSS attacks and the importance of sanitizing user input to prevent such vulnerabilities1234 Reference: https://ktflash.gitbooks.io/ceh_v9/content/125_countermeasures.html

NEW QUESTION # 134
.....

P.S. Free 2026 EC-COUNCIL 312-39 dumps are available on Google Drive shared by Exam4PDF: https://drive.google.com/open?id=1VkWLg0YaiaALac6cIYm7QTBYCJTaqISn