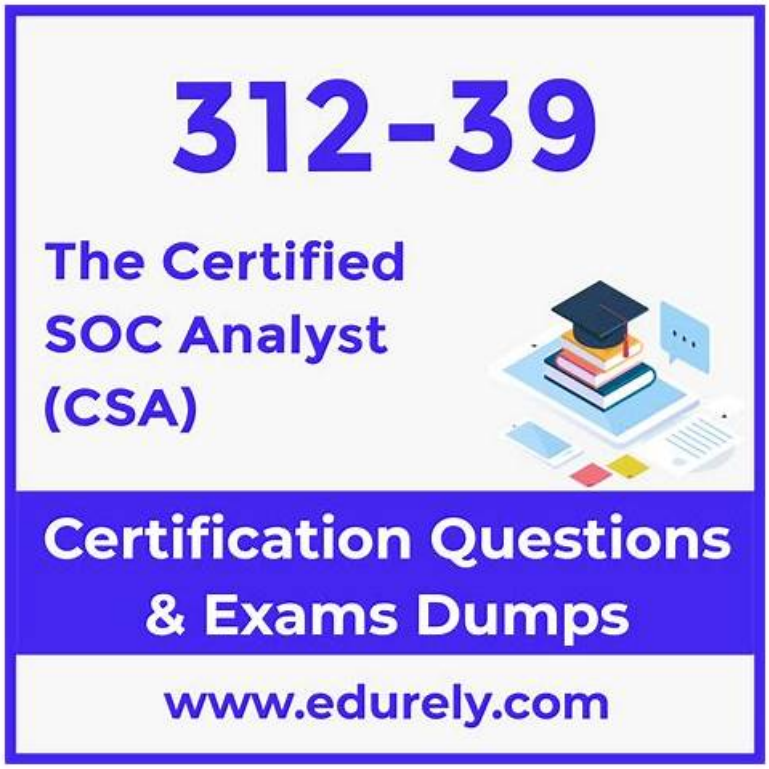
Pass Guaranteed EC-COUNCIL - Professional 312-39 - Certified SOC Analyst (CSA) Top Questions



2026 Latest PDFBraindumps 312-39 PDF Dumps and 312-39 Exam Engine Free Share: https://drive.google.com/open?id=1TEOsi0OpP8yUCnvERkpYnxvL1C0X6P9f

If you have any problems installing and using 312-39 study engine, you can contact our staff immediately. You know, we have so many users. If you do not immediately receive a link from us, you can send us an email to urge us. We hope you can use our 312-39 Exam simulating as soon as possible! Our system is very smooth and you basically have no trouble. We hope you enjoy using our 312-39 study engine.

Our Certified SOC Analyst (CSA) exam question has been widely praised by all of our customers in many countries and our company has become the leader in this field. Our product boost varied functions and they include the self-learning and the self-assessment functions, the timing function and the function to stimulate the exam to make you learn efficiently and easily. There are many advantages of our 312-39 Study Tool. If any questions or doubts exist, the client can contact our online customer service or send mails to contact us and we will solve them as quickly as we can. We always want to let the clients be satisfied and provide the best 312-39 test torrent and won't waste their money and energy.

>> 312-39 Top Questions <<

Valid Dumps 312-39 Free & Exam 312-39 Introduction

You may be also one of them, you may still struggling to find a high quality and high pass rate Certified SOC Analyst (CSA) study question to prepare for your exam. Your search will end here, because our study materials must meet your requirements. Our product is elaborately composed with major questions and answers. Our study materials are choosing the key from past materials to finish our 312-39 Torrent prep. It only takes you 20 hours to 30 hours to do the practice. After your effective practice, you can master the examination point from the 312-39 exam torrent. Then, you will have enough confidence to pass it. So start with our 312-39 torrent prep from now on. We can succeed so long as we make efforts for one thing.

The Certified SOC Analyst (CSA) certification exam is based on the EC-Council's CSA course, which covers a wide range of topics related to SOC operations. 312-39 course is designed to provide candidates with a comprehensive understanding of the tools, techniques, and processes used in SOC operations. Candidates who successfully pass the exam will be able to demonstrate

their ability to identify security incidents, analyze security logs, and respond to security incidents in a timely and effective manner.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q19-Q24):

NEW QUESTION # 19
Identify the event severity level in Windows logs for the events that are not necessarily significant, but may indicate a possible future problem.

- A. Information
- B. Failure Audit
- C. Error
- D. Warning

Answer: D

NEW QUESTION # 20
Which of the following security technology is used to attract and trap people who attempt unauthorized or illicit utilization of the host system?

- A. Intrusion Detection System
- B. De-Militarized Zone (DMZ)
- C. Honeypot
- D. Firewall

Answer: C

NEW QUESTION # 21
Jony, a security analyst, while monitoring IIS logs, identified events shown in the figure below.
What does this event log indicate?

- A. Parameter Tampering Attack
- B. SQL Injection Attack
- C. Directory Traversal Attack
- D. XSS Attack

Answer: B

Explanation:
TheIIS log events indicate a SQL Injection Attack. This is evident from the complex SQL queries present in the log, which include functions like "UNICODE", "SUBSTRING", and "MAX". These functions are being used in a manner that suggests manipulation of strings and extraction of data, which are common tactics in SQL injection attacks. The use of specific characters like CHAR(97) and CHAR(108) within the queries is a technique often employed to bypass security mechanisms during such attacks.
References: For further study and verification, the EC-Council's Certified SOC Analyst (CSA) course materials and study guides provide extensive information on identifying and responding to various types of cyber attacks, including SQL Injection. These resources are essential for any security analyst to understand the intricacies of log analysis and attack identification.

NEW QUESTION # 22
Which of the following is a correct flow of the stages in an incident handling and response (IH&R) process?

- A. Containment -> Incident Recording -> Incident Triage -> Preparation -> Recovery -> Eradication -> Post-Incident Activities
- B. Preparation -> Incident Recording -> Incident Triage -> Containment -> Eradication -> Recovery -> Post-Incident Activities
- C. Incident Triage -> Eradication -> Containment -> Incident Recording -> Preparation -> Recovery -> Post-Incident Activities
- D. Incident Recording -> Preparation -> Containment -> Incident Triage -> Recovery -> Eradication -> Post-Incident Activities

Answer: B

Explanation:
The correct flow of stages in an Incident Handling and Response (IH&R) process typically follows a structured approach that begins with Preparation, which is crucial for an effective response to incidents. This is followed by Incident Recording, where details of the incident are documented. Incident Triage is the next stage, where incidents are prioritized based on their impact. Containment strategies are then employed to limit the spread of the incident. Eradication involves removing the threat from the affected systems. Recovery is the process of restoring systems to normal operation. Finally, Post-Incident Activities involve learning from the incident and improving future response efforts.
References: The stages of the IH&R process are outlined in various EC-Council resources, including the EC-Council's Certified Incident Handler (E|CIH) program and related training materials, which emphasize the importance of a structured and methodical approach to incident handling and response123.

NEW QUESTION # 23
In which of the following incident handling and response stages, the root cause of the incident must be found from the forensic results?

- A. Systems Recovery
- B. Eradication
- C. Evidence Gathering
- D. Evidence Handling

Answer: C

NEW QUESTION # 24
.....

Because they are immensely useful and help you gain success in a 312-39 certification exam. More than ever, the professionals are now facing a highly competitive world to get their talent recognized enhancing their positions in their work environment. Such a milieu demands them to enrich their candidature more seriously. So the professionals work hard to maintain their quality and never fail in doing so. PDFBraindumps 312-39 Certification exams are the best option for any ambitious and ardent professional to make his continuation in his area of work intact.

poppiejpgc592453.elbloglibre.com, fatallisto.com, Disposable vapes

DOWNLOAD the newest PDFBraindumps 312-39 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1TEOsi0OpP8yUCnvERkpYnxvL1C0X6P9f