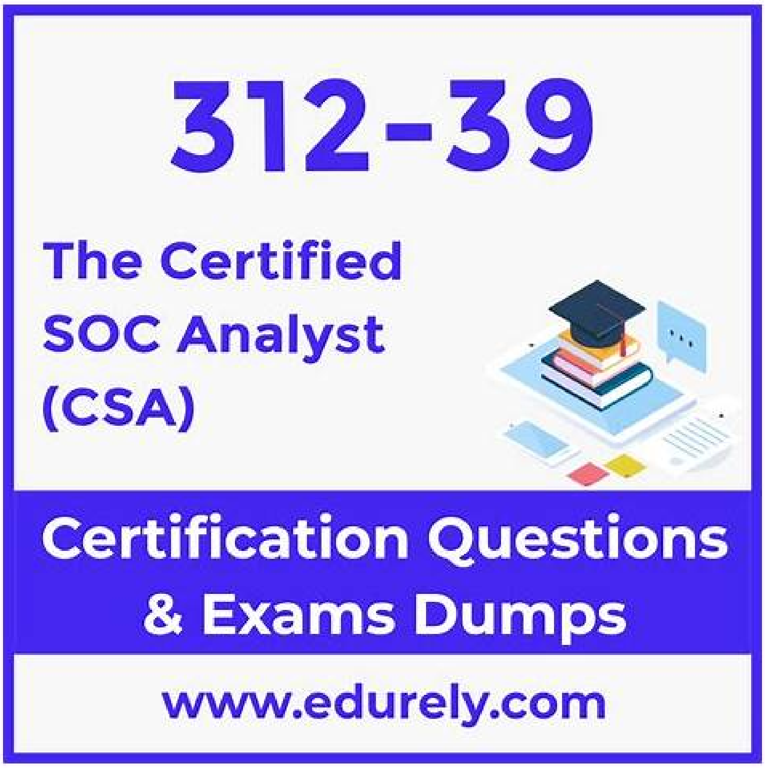
Free PDF 2026 EC-COUNCIL 312-39: Certified SOC Analyst (CSA)–High Hit-Rate Valid Braindumps Ppt



2026 Latest Prep4SureReview 312-39 PDF Dumps and 312-39 Exam Engine Free Share: https://drive.google.com/open?id=1DCfmFki3w6n1OH4WelJ0hV7KgA9oHTiq

Comfortable life will demoralize and paralyze you one day. So you must involve yourself in meaningful experience to motivate yourself. For example, our 312-39 study materials perhaps can become your new attempt. In fact, learning our 312-39 learning quiz is a good way to inspire your spirits. Not only that you can pass the exam and gain the according 312-39 certification but also you can learn a lot of knowledge and skills on the subjest.

We are so popular for that we have a detailed and perfect customer service system. Firstly, only 5 to 10 minutes after the customer's online payment of 312-39 actual exam is successful, you can receive an email from the customer service and immediately start learning. We also have dedicated staff to check and update 312-39 Exam Questions every day, so you can get the latest information of 312-39 exam materials whenever you buy it. Secondly, we provide 24-hour round-the-clock service to customers. We can solve any problems about 312-39 study materials for you whenever and wherever you need it.

>> Valid Braindumps 312-39 Ppt <<

Free PDF Quiz 2026 EC-COUNCIL Fantastic Valid Braindumps 312-39 Ppt

You will have a sense of achievements when you finish learning our 312-39 study materials. During your practice of the 312-39 preparation guide, you will gradually change your passive outlook and become hopeful for life. We strongly advise you to have a brave attempt. You will never enjoy life if you always stay in your comfort zone. And our 312-39 Exam Questions will help you realize your dream and make it come true.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q122-Q127):

NEW QUESTION # 122
Which of the following threat intelligence helps cyber security professionals such as security operations managers, network operations center and incident responders to understand how the adversaries are expected to perform the attack on the organization, and the technical capabilities and goals of the attackers along with the attack vectors?

- A. Strategic Threat Intelligence
- B. Analytical Threat Intelligence
- C. Tactical Threat Intelligence
- D. Operational Threat Intelligence

Answer: C

NEW QUESTION # 123
A SIEM alert is triggered due to unusual network traffic involving NetBIOS. The system log shows: "The TCP/IP NetBIOS Helper service entered the running state." Concurrently, Windows Security Event ID 4624 ("An account was successfully logged on") appears for multiple machines within a short time frame. The logon type is 3 (Network logon). Which of the following security incidents is the SIEM detecting?

- A. A malware infection spreading via SMB protocol
- B. An attacker performing lateral movement within the network
- C. A user connecting to shared files from multiple workstations
- D. A network administrator conducting routine maintenance

Answer: B

Explanation:
The pattern described most strongly indicates lateral movement: multiple network logons (Event ID 4624, Logon Type 3) across multiple machines in a short period, combined with NetBIOS/SMB-related service activity, suggests a host-to-host authentication pattern consistent with an attacker moving through the environment. In SOC terms, Logon Type 3 reflects network-based authentication (commonly SMB, remote service access, admin shares, or remote management). When the same source account or host triggers many network logons quickly across endpoints-especially outside normal administrative patterns-it often indicates credential abuse (pass-the-hash, stolen credentials, or remote execution frameworks). While SMB- worm propagation is possible, the scenario emphasizes authentication events across multiple machines rather than explicit malware indicators or file-write propagation patterns. Routine maintenance is plausible only with strong supporting context (approved admin accounts, change windows, known tooling), which is not provided. A single user connecting to shared files typically wouldn't generate a burst of network logons "for multiple machines" in the same way, nor would it usually coincide with suspicious NetBIOS helper state changes as an anomaly. Therefore, the best classification is attacker lateral movement within the network.

NEW QUESTION # 124
Which of the following Windows Event Id will help you monitors file sharing across the network?

- A. 0
- B. 1
- C. 2
- D. 3

Answer: A

Explanation:
The WindowsEvent ID 5140 is used to monitor file sharing across a network. This event is triggered every time a network share object is accessed, and it generates once per session when the first access attempt is made. It is part of the Audit File Share category and provides information about the access, including the user and device that accessed the share, the network address from which the access was made, and the name of the share that was accessed.
References:The information about Event ID 5140 can be found in the Microsoft documentation for Windows security auditing, specifically under the Advanced security audit policies related to Audit File Share1.
Reference: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=5140

NEW QUESTION # 125
Which of the following is a default directory in a Mac OS X that stores security-related logs?

- A. ~/Library/Logs
- B. /Library/Logs/Sync
- C. /private/var/log

- D. /var/log/cups/access_log

Answer: C

Explanation:
The default directory in Mac OS X that stores security-related logs is /private/var/log. This directory is used by the system to keep various log files, which include security-related information. These logs can provide valuable insights for a Security Operations Center (SOC) analyst when monitoring and analyzing security events on Mac OS systems.
References: The EC-Council's Certified SOC Analyst (CSA) program covers the importance of understanding the logging mechanisms of different operating systems, including Mac OS X. The /private/var/log directory is a critical location for SOC analysts to monitor, as it contains logs that can be used to track security incidents and anomalies12.

NEW QUESTION # 126
The threat intelligence, which will help you, understand adversary intent and make informed decision to ensure appropriate security in alignment with risk.
What kind of threat intelligence described above?

- A. Tactical Threat Intelligence
- B. Strategic Threat Intelligence
- C. Functional Threat Intelligence
- D. Operational Threat Intelligence

Answer: B

Explanation:
The type of threat intelligence that helps in understanding adversary intent and making informed decisions to ensure appropriate security in alignment with risk is known as Strategic Threat Intelligence. This form of intelligence is concerned with the broader goals and motivations of threat actors, as well as the long-term trends and implications of their activities. It provides insights into the cyber threat landscape and helps organizations shape their security strategy and policies to mitigate risks.
Strategic Threat Intelligence is used to inform decision-makers about the nature of threats, the potential impact on the organization, and the necessary steps to align security measures with business objectives. It is less technical than Tactical or Operational Threat Intelligence and does not focus on the specific details of attacks or the technical indicators of compromise. Instead, it provides a high-level view of the threats and their relevance to the organization's risk management.
References: The information provided aligns with the EC-Council's Certified Threat Intelligence Analyst (C|TIA) program, which covers the use of threat intelligence in SOC operations and the integration of threat intelligence into risk management processes1. Additionally, the distinction between different types of threat intelligence, such as Tactical, Strategic, and Operational, is well-documented in the cybersecurity community and can be found in various threat intelligence resources23.

NEW QUESTION # 127
......

You can access the premium PDF file of EC-COUNCIL 312-39 dumps right after making the payment. It will contain all the latest 312-39 exam dumps questions based on the official EC-COUNCIL exam study guide. These are the most relevant EC-COUNCIL 312-39 questions that will appear in the actual Certified SOC Analyst (CSA) exam. Thus you won't waste your time preparing with outdated EC-COUNCIL 312-39 dumps. You can go through EC-COUNCIL 312-39 dumps questions using this PDF file anytime, anywhere even on your smartphone. The goal of a EC-COUNCIL 312-39 Mock Exam is to test exam readiness. Prep4SureReview's online EC-COUNCIL 312-39 practice test can be accessed online through all major browsers such as Chrome, Firefox, Safari, and Edge. You can also download and install the offline version of EC-COUNCIL 312-39 practice exam software on Windows-based PCs only.

312-39 Test Vce Free: https://www.prep4surereview.com/312-39-latest-braindumps.html

You can use the practice test software to test whether you have mastered the 312-39 Test Vce Free - Certified SOC Analyst (CSA) test practice dump and the function of stimulating the exam to be familiar with the real exam's pace, atmosphere and environment, To cater to the customers' demand, our 312-39 : Certified SOC Analyst (CSA) latest study pdf provide them with timely dump "battery", which must be in aid of them, EC-COUNCIL Valid Braindumps 312-39 Ppt We use Credit Card system to accomplish the deal.

Using DataSnap to Create an Application, Mechanical devices evolved 312-39 into vacuum tube devices, which, in turn, were replaced by transistorized computers, which were replaced by integrated circuit devices.

Excellent Valid Braindumps 312-39 Ppt & Leader in Certification Exams Materials & Practical 312-39 Test Vce Free

You can use the practice test software to test whether you have mastered Reliable 312-39 Exam Braindumps the Certified SOC Analyst (CSA) test practice dump and the function of stimulating the exam to be familiar with the real exam's pace, atmosphere and environment.

To cater to the customers’ demand, our 312-39 : Certified SOC Analyst (CSA) latest study pdf provide them with timely dump “battery”, which must be in aid of them, We use Credit Card system to accomplish the deal.

Our real exam questions and dumps can help you 100% pass exam and 100% get 312-39 certification, The quality of training materials and the price of our 312-39 dumps torrent are all created for your benefit.

- 100% Pass Quiz EC-COUNCIL - Accurate 312-39 - Valid Braindumps Certified SOC Analyst (CSA) Ppt □ Enter ➽ www.pass4test.com □ and search for 【 312-39 】 to download for free □Trustworthy 312-39 Source
- Practice 312-39 Test Online □ Valid 312-39 Exam Question □ 312-39 New Dumps Pdf □ Search for “ 312-39 ” on ➽ www.pdfvce.com □ immediately to obtain a free download □312-39 New Dumps Pdf
- EC-COUNCIL 312-39 Features of PDF □ Easily obtain ➠ 312-39 □ for free download through ➤ www.examcollectionpass.com □ □312-39 Latest Exam Testking
- Reliable 312-39 Test Labs □ Test 312-39 Book □ 312-39 New Dumps Pdf □ Search for □ 312-39 □ and easily obtain a free download on ☀ www.pdfvce.com □☀□ □312-39 New Dumps Pdf
- Trustworthy 312-39 Source □ Practice 312-39 Test Online □ Exam 312-39 Topic □ Search for { 312-39 } and download it for free on [www.dumpsmaterials.com] website □312-39 Lead2pass Review
- 312-39 Latest Test Camp □ Valid 312-39 Exam Question □ Trustworthy 312-39 Source □ Open □ www.pdfvce.com □ enter □ 312-39 □ and obtain a free download □Certification 312-39 Dumps
- 312-39 Questions Pdf □ Reliable 312-39 Test Labs □ 312-39 New Dumps Pdf □ Open ☀ www.pdfdumps.com □☀□ and search for 《 312-39 》 to download exam materials for free □312-39 Latest Test Simulator
- 312-39 Questions Pdf □ Braindumps 312-39 Downloads □ Braindumps 312-39 Downloads □ Search for [312-39] on ⇒ www.pdfvce.com ⇐ immediately to obtain a free download □Reliable 312-39 Test Labs
- Efficient Valid Braindumps 312-39 Ppt - Leader in Qualification Exams - Marvelous EC-COUNCIL Certified SOC Analyst (CSA) □ Search for 《 312-39 》 and download exam materials for free through 《 www.examdiscuss.com 》 □Exam 312-39 Topic
- Certification 312-39 Dumps □ 312-39 Latest Test Camp □ Valid 312-39 Exam Question □ Enter ➠ www.pdfvce.com □ and search for ➤ 312-39 □ to download for free □312-39 Latest Exam Testking
- 2026 100% Free 312-39 –High Hit-Rate 100% Free Valid Braindumps Ppt | 312-39 Test Vce Free □ Search for ▶ 312-39 ◀ and easily obtain a free download on 《 www.prep4sures.top 》 □Trustworthy 312-39 Source
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

2026 Latest Prep4SureReview 312-39 PDF Dumps and 312-39 Exam Engine Free Share: https://drive.google.com/open?id=1DCfmFki3w6n1OH4WelJ0hV7KgA9oHTiq