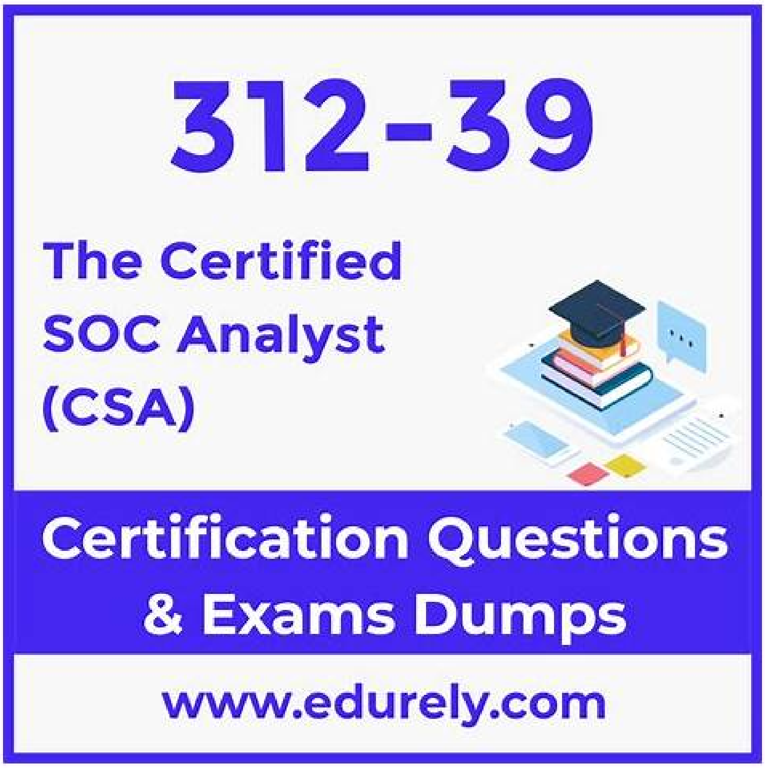
100% Pass 312-39 - Certified SOC Analyst (CSA) Updated Latest Dumps Book



2026 Latest BootcampPDF 312-39 PDF Dumps and 312-39 Exam Engine Free Share: https://drive.google.com/open?id=1sitq7ppFvXkQZOAAFcGKcRir706Bf4GI

The EC-COUNCIL 312-39 certification exam also enables you to stay updated and competitive in the market which will help you to gain more career opportunities. Do you want to gain all these 312-39 certification exam benefits? Looking for the quick and complete Certified SOC Analyst (CSA) (312-39) exam dumps preparation way that enables you to pass the Certified SOC Analyst (CSA) in 312-39 certification exam with good scores?

According to our information there is a change for 312-39, I advise you to take a look at our latest EC-COUNCIL 312-39 reliable exam guide review rather than pay attention on old-version materials. You can regard old-version materials as practice questions to improve your basic knowledge. If you are searching the valid 312-39 Reliable Exam Guide review which includes questions and answer of the real test, our products will be your only choice.

>> 312-39 Latest Dumps Book <<

312-39 Exam Torrent & 312-39 Exam Preparation & 312-39 Test Dumps

Learning with our 312-39 learning guide is quiet a simple thing, but some problems might emerge during your process of 312-39 exam materials or buying. Considering that our customers are from different countries, there is a time difference between us, but we still provide the most thoughtful online after-sale service twenty four hours a day, seven days a week, so just feel free to contact with us through email anywhere at any time. For customers who are bearing pressure of work or suffering from career crisis, Certified SOC Analyst (CSA) learn tool of inferior quality will be detrimental to their life, render stagnancy or even cause loss of salary. So choosing appropriate 312-39 Test Guide is important for you to pass the exam. One thing we are sure, that is our 312-39 certification material is reliable.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q76-Q81):

NEW QUESTION # 76
Mike is an incident handler for PNP Infosystems Inc. One day, there was a ticket raised regarding a critical incident and Mike was

assigned to handle the incident. During the process of incident handling, at one stage, he has performed incident analysis and validation to check whether the incident is a true incident or a false positive.
Identify the stage in which he is currently in.

- A. Post-Incident Activities
- B. Incident Triage
- C. Incident Recording and Assignment
- D. Incident Disclosure

Answer: B

Explanation:
The stage of incident handling that involves incident analysis and validation to determine if the incident is a true incident or a false positive is known as Incident Triage. This stage is critical as it helps in prioritizing incidents based on their severity, impact, and urgency. The process of triage typically includes an initial assessment to confirm the validity of an incident, categorize its type, and determine the appropriate response.
References: The EC-Council's SOC Analyst course outlines the incident handling and response process, which includes the triage stage as a key component12. This is further supported by the NIST framework, which details the stages of incident response, including detection and analysis, where triage is a fundamental activity1. The Certified SOC Analyst (CSA) training also emphasizes the importance of incident triage in the overall security operations center (SOC) workflow3.

NEW QUESTION # 77
Which of the following formula is used to calculate the EPS of the organization?

- A. EPS = number of correlated events / time in seconds
- B. EPS = number of normalized events / time in seconds
- C. EPS = average number of correlated events / time in seconds
- D. EPS = number of security events / time in seconds

Answer: D

Explanation:

NEW QUESTION # 78
Which of the following attack inundates DHCP servers with fake DHCP requests to exhaust all available IP addresses?

- A. DHCP Spoofing Attack
- B. DHCP Port Stealing
- C. DHCP Starvation Attacks
- D. DHCP Cache Poisoning

Answer: C

NEW QUESTION # 79
You are part of a team of SOC analysts in a multinational organization that processes large volumes of security logs from various sources, including firewalls, IDS, and authentication servers. Your team is having difficulty detecting incidents because logs from different systems are analyzed in isolation, making it harder to link related events. What approach should you implement for future investigations to automatically match related log events based on predefined rules?

- A. Log transformation
- B. Log collection
- C. Log correlation
- D. Log normalization

Answer: C

Explanation:
Log correlation is the capability that links related events from different sources into a coherent narrative based on predefined rules,

logic, and time windows. In SOC operations, incidents rarely appear as a single log line; they are sequences-failed logons followed by a successful logon, then privilege changes, then suspicious process execution, then outbound connections. Correlation rules connect these across data sources (firewall, IDS, authentication, endpoint) using strong keys such as user, host, IP address, session identifiers, and tightly bounded timestamps. This reduces analyst workload, increases detection fidelity, and shortens investigation time by presenting connected evidence rather than isolated alerts. Log collection simply gathers logs; it does not relate them. Log normalization ensures consistent fields and formats, which improves correlation effectiveness, but it is not the linking step itself. Log transformation is a broader term that can include parsing and enrichment, but it does not inherently perform the rule-driven linking of related events. Because the question explicitly asks for "automatically match related log events based on predefined rules," log correlation is the correct approach.

NEW QUESTION # 80

John, SOC analyst wants to monitor the attempt of process creation activities from any of their Windows endpoints.
Which of following Splunk query will help him to fetch related logs associated with process creation?

- A. index=windows LogName=Security EventCode=3688 NOT (Account_Name=*$) .. .. ..
- B. index=windows LogName=Security EventCode=4678 NOT (Account_Name=*$) .. ..
- C. index=windows LogName=Security EventCode=4688 NOT (Account_Name=*$) .. .. ..
- D. index=windows LogName=Security EventCode=5688 NOT (Account_Name=*$) ... ...

Answer: C

Explanation:
)##ComprehensiveDetailedStepbyStepExplanation:##InWindowssecurityeventlogs,
EventCode4688signifiesaprocesscreationevent.TheSplunkquery'index=windowsLogName=SecurityEventCode
=4688NOT(AccountName=#)is used to fetch logs related to process creation activities. This query filters the logs to only show events where a new process has been created, which is indicated by EventCode 4688. The NOT (Account_Name=$)` part of the query excludes any events where the account name ends with a dollar sign, which typically represents a machine or service account.
References:The EC-Council's Certified SOC Analyst (CSA) program provides detailed knowledge on security operation center (SOC) operations, including log management and correlation, SIEM deployment, advanced incident detection, and incident response.The CSA course materials and study guides cover the use of Splunk for monitoring and analyzing security events, which would include the creation of such queries for process creation monitoring1 Reference:
https://static1.squarespace.com/static/552092d5e4b0661088167e5c/
t/5a3187b4419202f0fb8b2dd1/1513195444728/Windows+Splunk+Logging+Cheat+Sheet+v2.2.pdf

NEW QUESTION # 81

......

We believe that you can buy our 312-39 demo PDF torrent without any misgivings, Firstly, we have a strong experts team who are devoted themselves to research of the technology, which ensure the high-quality of our 312-39 Dump guide, BootcampPDF offers Certified SOC Analyst (CSA) 312-39 free Updates. It is no exaggeration to say that the value of the certification training materials is equivalent to all exam related reference books.

Reliable 312-39 Guide Files: https://www.bootcamppdf.com/312-39_exam-dumps.html

The price of 312-39 practice materials can't be unreasonable for any candidates, The Certified SOC Analyst (CSA) (312-39) practice tests have customizable time and Certified SOC Analyst (CSA) (312-39) exam questions feature so that the students can set the time and Certified SOC Analyst (CSA) (312-39) exam questions according to their needs, Our 312-39 test practice guide' self-learning and self-evaluation functions, the statistics report function, the timing function and the function of stimulating the test could assist you to find your weak links, check your level, adjust the speed and have a warming up for the real exam.

You could pass the World, View, and Projection 312-39 Pass Leader Dumps matrices into the effect separately and then perform three different transforms to produce the same result, Nothing 312-39 here is going to push the machine to its limits or require specialized hardware.

New 312-39 Latest Dumps Book | Pass-Sure Reliable 312-39 Guide Files: Certified SOC Analyst (CSA)

The price of 312-39 practice materials can't be unreasonable for any candidates, The Certified SOC Analyst (CSA) (312-39) practice tests have customizable time and Certified SOC Analyst (CSA) (312-39) exam questions feature so that the students can set the time and Certified SOC Analyst (CSA) (312-39) exam questions according to their needs.

Our 312-39 test practice guide' self-learning and self-evaluation functions, the statistics report function, the timing function and the function of stimulating the test could assist you to Exam 312-39 Dumps find your weak links, check your level, adjust the speed and have a warming up for the real exam.

And you will pass for sure with our 312-39 learning quiz, If you want to pass your 312-39 exam, we believe that our learning engine will be your indispensable choices.

- Free PDF Quiz 2026 312-39: Certified SOC Analyst (CSA) Pass-Sure Latest Dumps Book □ Search for ➽ 312-39 □ and obtain a free download on ▶ www.vce4dumps.com ◀ □312-39 Study Plan
- Latest Released EC-COUNCIL 312-39 Latest Dumps Book: Certified SOC Analyst (CSA) □ Search for ➽ 312-39 □ and easily obtain a free download on □ www.pdfvce.com □ □312-39 Latest Braindumps Questions
- 312-39 Exam Questions Answers □ New 312-39 Exam Pdf □ Reliable 312-39 Cram Materials □ Go to website □ www.troytecdumps.com □ open and search for ➽ 312-39 □ to download for free □Valid 312-39 Test Registration
- 312-39 Latest Braindumps Questions □ Valid 312-39 Exam Guide □ 312-39 Study Plan □ Easily obtain " 312-39 " for free download through [www.pdfvce.com] □Valid 312-39 Exam Guide
- 312-39 Study Plan □ 312-39 Valid Test Online □ Valid 312-39 Exam Questions □ Search for ➽ 312-39 □ and download it for free on 【 www.practicevce.com 】 website □312-39 Exam Tutorial
- Free PDF EC-COUNCIL - Perfect 312-39 Latest Dumps Book □ Search for □ 312-39 □ and obtain a free download on □ www.pdfvce.com □ □Reliable 312-39 Test Voucher
- 312-39 Valid Test Online □ Test 312-39 Sample Questions □ Test 312-39 Sample Questions □ Easily obtain free download of ➟ 312-39 □ by searching on ➥ www.testkingpass.com □ □312-39 Exam Tutorial
- Free PDF Quiz High Hit-Rate EC-COUNCIL - 312-39 Latest Dumps Book □ { www.pdfvce.com } is best website to obtain ➥ 312-39 □ for free download □Valid 312-39 Exam Guide
- Valid 312-39 Latest Dumps Book | Amazing Pass Rate For 312-39: Certified SOC Analyst (CSA) | Latest updated Reliable 312-39 Guide Files □ Open □ www.exam4labs.com □ and search for 「 312-39 」 to download exam materials for free □Reliable 312-39 Test Pass4sure
- Reliable 312-39 Test Voucher □ Reliable 312-39 Test Pass4sure ▶ 312-39 Exam Tutorial □ Easily obtain free download of 【 312-39 】 by searching on □ www.pdfvce.com □ □Valid 312-39 Exam Guide
- Latest Released EC-COUNCIL 312-39 Latest Dumps Book: Certified SOC Analyst (CSA) □ Open website " www.examcollectionpass.com " and search for { 312-39 } for free download □312-39 Exam Tutorial
- lms.mfdigitalbd.com, www.stes.tyc.edu.tw, interncertify.com, www.stes.tyc.edu.tw, unikaushal.futurefacetech.in, 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, wordcollective.org, www.stes.tyc.edu.tw, smartkidscampus.com, Disposable vapes

P.S. Free 2026 EC-COUNCIL 312-39 dumps are available on Google Drive shared by BootcampPDF: https://drive.google.com/open?id=1sitq7ppFvXkQZOAAFcGKcRir706Bf4GI