EC-COUNCIL 312-39 New Study Guide & Exam 312-39 Vce

BTW, DOWNLOAD part of Lead2Passed 312-39 dumps from Cloud Storage: https://drive.google.com/open?id=1mvyhOrntKzdMCH0HiypWj93UkyILbt8f

The quality of our 312-39 exam questions is very high and we can guarantee to you that you will have no difficulty to pass the exam. The content of the questions and answers of 312-39 study braindumps is refined and focuses on the most important information. To let the clients be familiar with the atmosphere and pace of the real exam we provide the function of stimulating the exam. Our expert team updates the 312-39 training guide frequently to let the clients practice more. Every detail of our 312-39 learning prep is perfect.

The Certified SOC Analyst (CSA) certification is offered by the International Council of E-Commerce Consultants (EC-Council) as a way for professionals in the cybersecurity industry to demonstrate their knowledge and skills in the area of Security Operations Centers (SOCs). Certified SOC Analyst (CSA) certification is designed for individuals who are responsible for detecting, analyzing, and responding to cybersecurity incidents within an organization.

>> EC-COUNCIL 312-39 New Study Guide <<

Pass Guaranteed Quiz 312-39 - Certified SOC Analyst (CSA) –The Best New Study Guide

The Lead2Passed is a leading platform that is committed to ace the EC-COUNCIL 312-39 exam preparation and enabling the candidates to pass the final Certified SOC Analyst (CSA) (312-39) exam easily. To achieve this objective the Lead2Passed is offering real and updated EC-COUNCIL Certifications 312-39 Exam Questions. These EC-COUNCIL 312-39 exam questions are designed and verified by qualified 312-39 subject matter experts.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q189-Q194):

NEW QUESTION # 189
Pearl is a Level 1 SOC analyst at a global financial institution using SQL Server to store sensitive customer information. She investigates an alert showing multiple failed web app logins from the same IP, followed by a successful login as a server

administrator. She then reviews SQL Server logs and finds the attacker used compromised credentials to access the SQL Server database. Which log will help identify whether the intruder performed unauthorized modifications in the database?

- A. Transaction log
- B. Security log
- C. Maintenance log
- D. Audit log

Answer: A

Explanation:
The SQL Server transaction log records changes made to the database, including data modifications (INSERT /UPDATE/DELETE) and many schema-related operations, supporting reconstruction of what changed and when. For unauthorized modifications, the transaction log provides the strongest evidence trail because it is tied to the database engine's durability mechanism and captures the sequence of committed actions. In SOC investigations, transaction log analysis helps determine whether data was altered, which tables were impacted, and the time window of changes. Security logs or SQL Server security-related events help with authentication
/authorization and may show login activity, but they do not reliably enumerate every data modification.
Maintenance logs relate to scheduled maintenance tasks (backups, index rebuilds) and are not designed to capture unauthorized content changes. Audit logs can be extremely useful if SQL Server auditing is configured to capture specific actions and statements, but the question asks which log helps identify whether modifications occurred; the transaction log is the baseline record of actual database changes. In practice, SOC teams correlate transaction log evidence with authentication logs, application logs, and potentially SQL auditing to attribute actions to accounts and sessions, then scope and remediate.

NEW QUESTION # 190
What does HTTPS Status code 403 represents?

- A. Not Found Error
- B. Unauthorized Error
- C. Forbidden Error
- D. Internal Server Error

Answer: C

Explanation:
The HTTPS status code 403 represents a Forbidden Error. This error occurs when the server understands the request but refuses to authorize it. Unlike the Unauthorized Error (401), which suggests that the request might be authorized if the client re-authenticates, the Forbidden Error indicates that re-authenticating will make no difference and access is denied regardless of authentication status. The Forbidden Error is tied to the application logic, such as insufficient rights to a resource or the server being programmed to deny access to a particular resource to the client. It is not related to the client's credentials but rather to the permissions set by the server for the requested resource.
References: The EC-Council SOC Analyst course materials and study guides discuss various HTTP status codes as part of understanding web application security and interpreting web logs within a Security Operations Center (SOC) context. The materials explain the meaning of the 403 Forbidden Error and its implications for cybersecurity analysis123.
Reference: https://en.wikipedia.org/wiki/HTTP_403

NEW QUESTION # 191
Which of the following is a set of standard guidelines for ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection?

- A. FISMA
- B. DARPA
- C. PCI-DSS
- D. HIPAA

Answer: C

NEW QUESTION # 192

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

Answer: D

NEW QUESTION # 193
What does Windows event ID 4740 indicate?

- A. A user account was enabled.
- B. A user account was locked out.
- C. A user account was created.
- D. A user account was disabled.

Answer: B

NEW QUESTION # 194
.....

Our valid EC-COUNCIL 312-39 dumps make the preparation easier for you. With these real 312-39 Questions, you can prepare for the test while sitting on a couch in your lounge. Whether you are at home or traveling anywhere, you can do 312-39 exam preparation with our EC-COUNCIL 312-39 Dumps. Certified SOC Analyst (CSA) (312-39) test candidates with different learning needs can use our three formats to meet their needs and prepare for 312-39 test successfully in one go. Read on to check out the features of these three formats.

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, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New 312-39 dumps are available on Google Drive shared by Lead2Passed: https://drive.google.com/open?id=1mvyhOrntKzdMCH0HiypWj93UkyILbt8f