EC-COUNCIL 312-39 Valid Test Vce Free - 312-39 Test Discount

2026 Latest PDFVCE 312-39 PDF Dumps and 312-39 Exam Engine Free Share: https://drive.google.com/open?id=14K6k2e023OM0XZjim7hCwOSolxyvukIc

The EC-COUNCIL 312-39 practice exam material is available in three different formats i.e EC-COUNCIL 312-39 dumps PDF format, web-based practice test software, and desktop 312-39 practice exam software. PDF format is pretty much easy to use for the ones who always have their smart devices and love to prepare for 312-39 Exam from them. Applicants can also make notes of printed Certified SOC Analyst (CSA) (312-39) exam material so they can use it anywhere in order to pass EC-COUNCIL 312-39 Certification with a good score.

The 312-39 Exam is a challenging and comprehensive certification exam that requires candidates to have a deep understanding of security operations center analysis. To prepare for the exam, candidates can take EC-COUNCIL's official training course or use other study materials such as practice exams, study guides, and online forums. Passing the CSA certification exam requires dedication and hard work, but it is a rewarding achievement that can open up new career opportunities in the cybersecurity field.

>> EC-COUNCIL 312-39 Valid Test Vce Free <<

312-39 Test Discount | 312-39 Pass Guarantee

If you follow the steps of our 312-39 exam questions, you can easily and happily learn and ultimately succeed in the ocean of learning. And our 312-39 exam questions can help you pass the 312-39 exam for sure. Choosing our 312-39 exam questions actually means that you will have more opportunities to be promoted in the near future. We are confident that in the future, our 312-39 Study Tool will be more attractive and the pass rate will be further enhanced. For now, the high pass rate of our 312-39 exam questions is more than 98%.

The CSA exam is a comprehensive test that covers a wide range of topics related to SOC operations. 312-39 Exam consists of 100 multiple-choice questions and has a time limit of four hours. The topics covered in the exam include threat intelligence, security incident management, network and endpoint monitoring, and incident response procedures.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q49-Q54):

NEW QUESTION # 49
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=*$) .. .. ..
- B. index=windows LogName=Security EventCode=5688 NOT (Account_Name=*$) ... ...
- C. index=windows LogName=Security EventCode=4688 NOT (Account_Name=*$) .. .. ..
- D. index=windows LogName=Security EventCode=4678 NOT (Account_Name=*$) .. ..

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 # 50
A financial institution suspects an insider threat due to unauthorized access attempts on restricted databases.
However, SIEM alerts lack sufficient information to differentiate between legitimate and malicious access.
The SOC manager recommends integrating contextual data to improve detection. Which contextual data source should be integrated in this scenario?

- A. Location and physical context from CPS sensors
- B. Threat context from external threat intelligence feeds
- C. Vulnerability context
- D. User context from HR systems

Answer: D

Explanation:
User context from HR systems is the most relevant contextual source for insider-threat differentiation because it helps determine whether access aligns with the user's role, employment status, and business need. HR context can include department, job title, manager, location assignment, employment status (active
/terminated), and sometimes risk signals like recent role changes or offboarding timelines. For restricted database access, the key questions are "should this person have access?" and "is this behavior normal for their role?" Threat intelligence feeds primarily help with external adversaries (malicious IPs, domains, known actor infrastructure) and are less useful for insiders who operate from legitimate networks and accounts.
Vulnerability context is useful for exposure management and exploit prioritization, but it doesn't explain whether a particular employee's access attempt is legitimate. Physical/CPS sensor context can be valuable in some environments (badge access vs. login), but the most broadly applicable and directly relevant enrichment for insider cases is HR-based identity context. In SOC operations, combining HR context with identity logs and data access telemetry improves detection logic (for example, flagging restricted access attempts by users outside the relevant business unit or after termination) and reduces false positives from legitimate administrative activity.

NEW QUESTION # 51
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. Operational Threat Intelligence

- C. Strategic Threat Intelligence
- D. Functional Threat Intelligence

Answer: C

NEW QUESTION # 52
Which of the following stage executed after identifying the required event sources?

- A. Implementing and Testing the Use Case
- B. Defining Rule for the Use Case
- C. Identifying the monitoring Requirements
- D. Validating the event source against monitoring requirement

Answer: D

NEW QUESTION # 53
An attacker exploits the logic validation mechanisms of an e-commerce website. He successfully purchases a product worth $100 for $10 by modifying the URL exchanged between the client and the server.
Original
URL: http://www.buyonline.com/product.aspx?profile=12
&debit=100
Modified URL: http://www.buyonline.com/product.aspx?profile=12
&debit=10
Identify the attack depicted in the above scenario.

- A. SQL Injection Attack
- B. Parameter Tampering Attack
- C. Session Fixation Attack
- D. Denial-of-Service Attack

Answer: B

Explanation:

NEW QUESTION # 54
.....

www.prep4away.com ◀ open and search for ▶ 312-39 ◀ to download for free Answers 312-39 Free

- 2026 Unparalleled EC-COUNCIL 312-39 Valid Test Vce Free Download （ 312-39 ） for free by simply entering 【 www.pdfvce.com 】 website ⛄312-39 Latest Dumps Ppt
- Why do you need to get help from www.vce4dumps.com EC-COUNCIL 312-39 Exam Questions? Download [312-39] for free by simply searching on ▶ www.vce4dumps.com ◀ 312-39 Latest Exam Registration
- myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

2026 Latest PDFVCE 312-39 PDF Dumps and 312-39 Exam Engine Free Share: https://drive.google.com/open?id=14K6k2e023OM0XZjim7hCwOSolxyvukIc