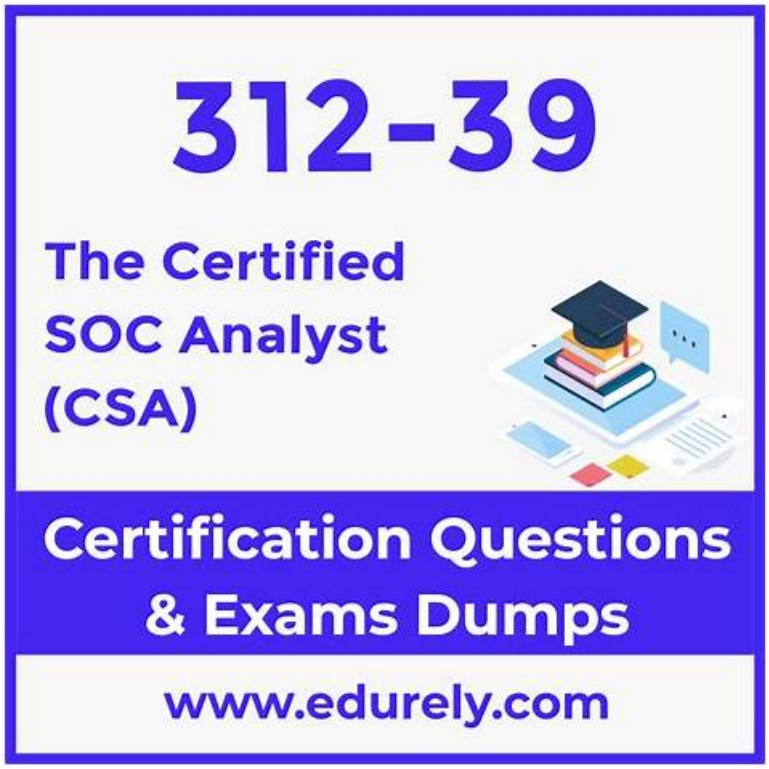
New 312-39 Test Vce Will Be Your Reliable Support to Pass Certified SOC Analyst (CSA)



BONUS!!! Download part of ActualCollection 312-39 dumps for free: https://drive.google.com/open?id=1nw_3ySbCc9X4j0bzzjdkFnC70xewvHWe

The 312-39 PDF is the collection of real, valid, and updated Certified SOC Analyst (CSA) (312-39) practice questions. The EC-COUNCIL 312-39 PDF dumps file works with all smart devices. You can use the 312-39 PDF questions on your tablet, smartphone, or laptop and start 312-39 Exam Preparation anytime and anywhere. The 312-39 dumps PDF provides you with everything that you must need in 312-39 exam preparation and enable you to crack the final 312-39 exam quickly.

EC-COUNCIL 312-39 Certified SOC Analyst (CSA) is a specialized certification that is designed for IT security professionals who want to master the art of identifying, analyzing, and mitigating security threats within a Security Operations Center (SOC) environment. Certified SOC Analyst (CSA) certification is globally recognized and is ideal for those who want to enhance their skills in the field of cybersecurity.

>> New 312-39 Test Vce <<

312-39 Updated Dumps, Online 312-39 Training Materials

For candidates who are going to buy 312-39 exam materials online, they may pay more attention to the website safety. We have technicians to examine the website at times, therefore we will offer you clean and safe online shopping environment if you choose us. In addition, we have a professional team to collect the first-hand information for 312-39 Exam Braindumps, and if you choose us, we can ensure that you can obtain the latest information for the exam. You can enjoy the free update for one year for 312-39 training materials, and the update version will be sent to you automatically.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q116-Q121):

NEW QUESTION # 116
InfoSystem LLC, a US-based company, is establishing an in-house SOC. John has been given the responsibility to finalize strategy, policies, and procedures for the SOC.
Identify the job role of John.

- A. Security Analyst - L2
- B. Security Analyst - L1
- C. Chief Information Security Officer (CISO)
- D. Security Engineer

Answer: C

Explanation:
The role of finalizing strategy, policies, and procedures for a Security Operations Center (SOC) typically falls under the responsibilities of a Chief Information Security Officer (CISO). The CISO is a senior-level executive within an organization who coordinates and manages the overall strategy and defense mechanisms to protect the organization's information and technology assets. This role involves leadership and strategic decision-making, which includes establishing the SOC's framework, defining its policies, and overseeing its procedures.
References: The EC-Council provides various resources and guides that outline the roles and responsibilities within a SOC. According to the information available, a Security Analyst, whether Level 1 or Level 2, is primarily responsible for monitoring and analyzing the organization's security posture on a continuous basis.
A Security Engineer focuses on the design and implementation of security systems. In contrast, the CISO role encompasses a broader scope of strategic leadership and management, which aligns with the responsibilities described for John in the scenario12.

NEW QUESTION # 117
During routine monitoring, the SIEM detects an unusual spike in outbound data transfer from a critical database server. The typical outbound traffic for this server is around 5 MB/hour, but in the past 10 minutes, it has sent over 500 MB to an external IP address. No predefined signatures match this activity, but the SIEM raises an alert due to deviations from the server's normal behavior profile. Which detection method is responsible for this alert?

- A. Rule-based detection
- B. Heuristic-based detection
- C. Anomaly-based detection
- D. Signature-based detection

Answer: C

Explanation:
This alert is generated because the activity deviates significantly from the server's established baseline, which is the hallmark of anomaly-based detection. The SIEM is not matching a known signature (so it is not signature-based), and the prompt emphasizes "deviations from normal behavior profile," which typically means statistical profiling, baselining, or behavior analytics detecting outliers in volume, timing, destination, or frequency. While rule-based detections can also trigger on thresholds, the question explicitly frames the logic as "normal behavior profile," which implies adaptive baselines rather than a fixed rule alone. Heuristic detection refers to generalized patterns or suspicion scoring, but here the core mechanism is abnormality versus historical norms (5 MB/hour typical vs 500 MB in 10 minutes). From a SOC triage perspective, anomaly alerts require quick validation: confirm the external destination reputation/ownership, verify whether the transfer aligns with authorized jobs, check change tickets, and correlate with authentication/process activity on the database host. Anomaly-based detection is especially valuable for data exfiltration because attackers can avoid known signatures, but they often struggle to mimic normal data movement patterns at scale.

NEW QUESTION # 118
Lisa Carter, a SOC analyst at a financial services firm, is performing a risk assessment following suspicious alerts detected by the SIEM. She evaluates three key factors: the likelihood of an attack succeeding based on current threat intelligence, the impact on critical business operations if the breach occurs, and the value of the assets targeted (e.g., customer data, financial systems). Using the standard risk assessment approach, which scenario represents the highest risk to the organization?

- A. High Likelihood, High Impact, High Asset Value
- B. Low Likelihood, Low Impact, High Asset Value
- C. Low Likelihood, High Impact, Low Asset Value
- D. High Likelihood, Low Impact, High Asset Value

Answer: A

Explanation:
The highest risk is the scenario where all contributing factors are high: likelihood, impact, and asset value.

Risk is commonly treated as a function of probability and consequence; many organizations also incorporate asset value or criticality into consequence. When likelihood is high, the threat is more probable to materialize.
When impact is high, the organization faces significant operational disruption, financial loss, and regulatory exposure. When asset value is high, the target represents highly sensitive or business-critical data/systems, which amplifies both the harm and urgency. Therefore, "High Likelihood, High Impact, High Asset Value" clearly produces the maximum risk rating. The other scenarios reduce at least one dimension: low likelihood reduces probability, low impact reduces consequence, and low asset value reduces business criticality and potential damage. In SOC practice, the highest-risk scenario drives immediate prioritization: faster containment, more aggressive monitoring, executive visibility, and resourcing for incident response. It also influences long-term control investments (identity hardening, segmentation, monitoring coverage, and detection engineering) because it represents the greatest potential harm combined with high probability.

NEW QUESTION # 119
Which of the following is a report writing tool that will help incident handlers to generate efficient reports on detected incidents during incident response process?

- A. Malstrom
- B. threat_note
- C. MagicTree
- D. IntelMQ

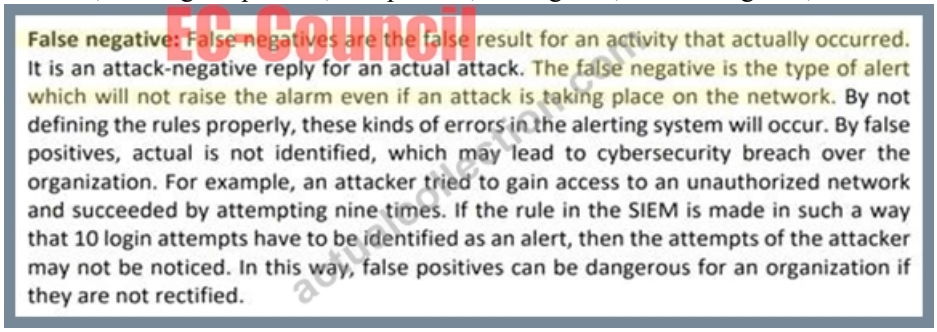
Answer: D

NEW QUESTION # 120
David is a SOC analyst in Karen Tech. One day an attack is initiated by the intruders but David was not able to find any suspicious events.
This type of incident is categorized into?

- A. False Negative Incidents
- B. True Positive Incidents
- C. True Negative Incidents
- D. False positive Incidents

Answer: A

Explanation:
A false negative incident in the context of a Security Operations Center (SOC) is when an actual attack or intrusion occurs, but the SOC analyst fails to detect any suspicious events or indicators of compromise. This means that the security measures in place did not work as intended, and the attack went unnoticed.
In David's case, since an attack was initiated and he was not able to find any suspicious events, it is categorized as a false negative incident. This is a critical type of incident because it indicates a failure in the detection capabilities of the SOC, potentially allowing the intruder to cause harm without being detected.
References: The categorization of incidents is a fundamental part of the SOC Analyst's role, as outlined in the EC-Council's Certified SOC Analyst (CSA) training and certification program. The program covers the different types of incidents that can be encountered in a SOC, including true positives, false positives, true negatives, and false negatives, and how to identify and respond to each12345.



NEW QUESTION # 121
.....

To attain this you just need to enroll in the 312-39 certification exam and put all your efforts to pass this challenging 312-39 exam with good scores. However, to get success in EC-COUNCIL 312-39 dumps PDF is not an easy task, it is quite difficult to pass it. But with proper planning, firm commitment, and EC-COUNCIL 312-39 Exam Questions, you can pass this milestone easily. The ActualCollection is a leading platform that offers real, valid, and updated EC-COUNCIL 312-39 Dumps.

312-39 Updated Dumps: https://www.actualcollection.com/312-39-exam-questions.html

- Professional New 312-39 Test Vce - Fantastic 312-39 Exam Tool Guarantee Purchasing Safety □ Open ✔ www.practicevce.com □✔□ and search for ⇛ 312-39 ⇚ to download exam materials for free □New 312-39 Mock Exam
- New 312-39 Test Vce - Quiz 2026 EC-COUNCIL Certified SOC Analyst (CSA) Realistic Updated Dumps □ Search for ➥ 312-39 □ and download exam materials for free through □ www.pdfvce.com □ □Latest 312-39 Exam Pass4sure
- New 312-39 Braindumps Sheet □ New 312-39 Mock Exam □ 312-39 Study Test □ Immediately open □ www.pdfdumps.com □ and search for （ 312-39 ） to obtain a free download □New 312-39 Mock Exam
- 312-39 Real Braindumps □ 312-39 Latest Braindumps Questions □ Latest 312-39 Exam Pass4sure □ Copy URL ▹ www.pdfvce.com ◃ open and search for □ 312-39 □ to download for free □New 312-39 Braindumps Sheet
- 312-39 Certification Sample Questions □ 312-39 Certification Sample Questions □ 312-39 Valid Test Syllabus □ The page for free download of □ 312-39 □ on 「 www.troytecdumps.com 」 will open immediately □312-39 Latest Practice Questions
- Buy EC-COUNCIL 312-39 Real Exam Dumps Today and Get Massive Benefits □ Search on ➠ www.pdfvce.com □ for 《 312-39 》 to obtain exam materials for free download □312-39 Certification Sample Questions
- 312-39 Latest Braindumps Questions □ 312-39 Study Test ❊ Exam 312-39 Bootcamp □ Go to website 「 www.practicevce.com 」 open and search for [312-39] to download for free □Exam 312-39 Bootcamp
- Latest 312-39 Exam Pass4sure □ 312-39 Dumps Download □ New 312-39 Braindumps Sheet □ Download ▸ 312-39 ◂ for free by simply searching on ☀ www.pdfvce.com □☀□ □Latest 312-39 Exam Pass4sure
- Free PDF 2026 High Hit-Rate 312-39: New Certified SOC Analyst (CSA) Test Vce □ Easily obtain free download of □ 312-39 □ by searching on “ www.verifieddumps.com ” □312-39 Exam Format
- Professional New 312-39 Test Vce - Fantastic 312-39 Exam Tool Guarantee Purchasing Safety □ Easily obtain free download of □ 312-39 □ by searching on ➠ www.pdfvce.com □ □Exam 312-39 Collection Pdf
- Real EC-COUNCIL 312-39 In PDF Document Prepare Exam get successful □ Enter ➤ www.examdiscuss.com □ and search for ✔ 312-39 □✔□ to download for free □312-39 Exam Cost
- socialislife.com, www.stes.tyc.edu.tw, safaqtxz152783.mdkblog.com, pennyaegd676467.59bloggers.com, directory-webs.com, alvineojn534274.blogsuperapp.com, brendasgtq820850.evawiki.com, jaysonfccx995437.theobloggers.com, jasperrfwa950630.blogtov.com, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New 312-39 dumps are available on Google Drive shared by ActualCollection: https://drive.google.com/open?id=1nw_3ySbCc9X4j0bzzjdkFnC70xewvHWe