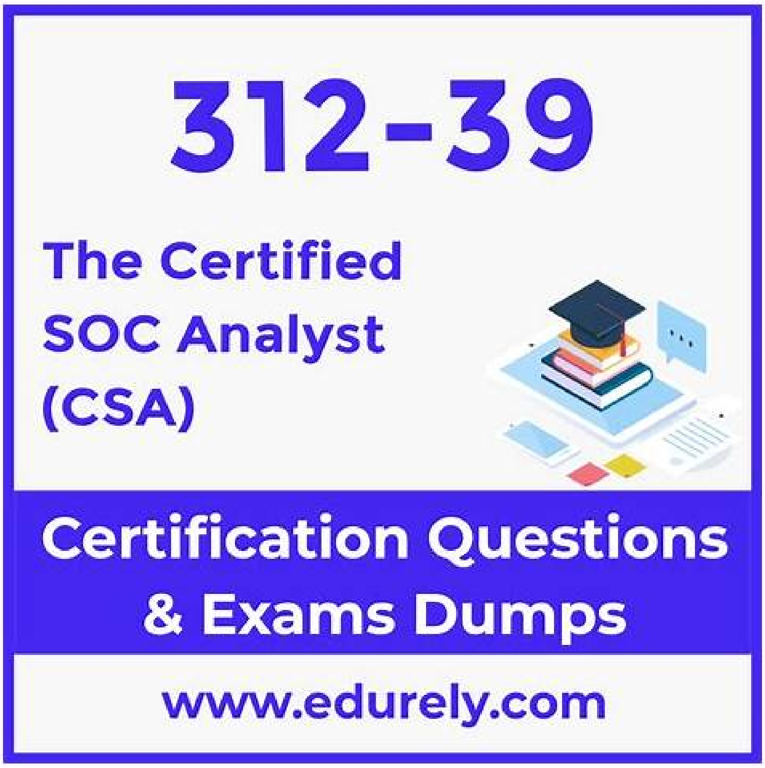
# Free PDF Quiz 2026 EC-COUNCIL 312-39: Certified SOC Analyst (CSA)–Trustable Valid Exam Camp



BONUS!!! Download part of ValidExam 312-39 dumps for free: https://drive.google.com/open?id=1cR6JvtiW7Fex9stGcmpcEJkqD5Y9lvlg

Our passing rate of 312-39 exam guide is 98%-100% and our 312-39 test prep can guarantee that you can pass the exam easily and successfully. Our 312-39 exam materials are highly efficient and useful and can help you pass the exam in a short time and save your time and energy. It is worthy for you to buy our 312-39 Quiz torrent and you can trust our product. You needn't worry about anything as long as you have our 312-39 training material. We guarantee to you our 312-39 exam materials can help you and you will have an extremely high possibility to pass the exam.

To prepare for the CSA exam, candidates can take advantage of a variety of training resources offered by EC-COUNCIL, including online courses, study guides, and practice exams. It is also recommended that candidates have practical experience in SOC analysis or a related field before taking the exam. Certified SOC Analyst (CSA) certification has a validity period of three years, after which individuals must recertify to maintain their credential.

The CSA certification is an intermediate-level certification that is ideal for professionals who are looking to advance their career in the cybersecurity field. It is particularly relevant for those who work in SOC environments, such as security analysts, incident responders, and SOC managers.

EC-COUNCIL 312-39 Certification Exam, also known as the Certified SOC Analyst (CSA) exam, is a professional certification exam that measures a candidate's knowledge and skills in the field of cybersecurity. 312-39 exam is designed to test an individual's ability to effectively monitor and defend against cyber threats in a Security Operations Center (SOC) environment.

**>> Valid 312-39 Exam Camp <<**

## New 312-39 Test Discount | 312-39 Reliable Test Vce

The PDF version of our 312-39 practice guide is convenient for reading and supports the printing of our study materials. If client uses the PDF version of 312-39 learning questions they can download the demos freely. If clients feel good after trying out our demos they will choose the full version of 312-39 training test bank to learn our study materials. The PDF version of our 312-39 study materials can be printed into paper documents and convenient for the client to take notes.

# EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q74-Q79):

**NEW QUESTION # 74**

Which of the following security technology is used to attract and trap people who attempt unauthorized or illicit utilization of the host system?

- A. Intrusion Detection System
- B. Honeypot
- C. Firewall
- D. De-Militarized Zone (DMZ)

**Answer: B**

Explanation:
A honeypot is a security mechanism that serves as a decoy to attract and trap individuals attempting unauthorized or illicit activities. It is designed to mimic a real system that appears vulnerable and valuable to attackers. The primary purpose of a honeypot is to distract attackers from legitimate targets, gather intelligence on attack strategies and behavior, and ultimately improve the overall security posture by learning from the attacks it captures.
* Attraction: The honeypot presents itself as an attractive target to potential attackers by simulating vulnerabilities.
* Engagement: Once the attackers engage with the honeypot, their activities are monitored and logged without their knowledge.
* Analysis: The data collected from these interactions is then analyzed to understand attack patterns, techniques, and goals.
* Improvement: This intelligence is used to enhance security measures, such as updating firewall rules or improving intrusion detection systems.
References:
* The EC-Council's Certified SOC Analyst (CSA) program includes training on various security
* technologies, including honeypots, as part of its curriculum to prepare individuals for roles in Security Operations Centers (SOC)1.
* EC-Council's resources on cybersecurity also provide detailed explanations of honeypots, their purposes, and their implementation within a cybersecurity framework2.
* Additionally, the role of a SOC Analyst often involves understanding and potentially deploying honeypots as part of a broader security strategy3.

**NEW QUESTION # 75**

A financial institution's SIEM is generating a high number of false positives, causing alert fatigue among SOC analysts. To reduce this burden and improve threat detection accuracy, the organization integrates AI capabilities into the SIEM. After implementation, the SOC team observes a significant decrease in redundant alerts, along with faster detection of genuine threats. Which AI capability contributed to this improvement?

- A. Data integration enhancement
- B. Automated rule generation
- C. Dynamic rule optimization
- D. Rule validation and testing

**Answer: C**

Explanation:
Dynamic rule optimization best explains a reduction in false positives and redundant alerts after adding AI to a SIEM. In SOC operations, alert fatigue often comes from static thresholds, overly broad correlations, and detections that don't adapt to changing baselines (new business apps, seasonal activity, infrastructure changes). AI-driven dynamic optimization can tune thresholds, suppress noisy patterns, and adjust scoring based on context (user role, device posture, known maintenance windows, historical behavior). This reduces duplicate/low-value alerts while preserving or improving sensitivity for real threats, which aligns with "decrease in redundant alerts" and "faster detection of genuine threats." Rule validation/testing improves quality but is usually a manual or pre-deployment activity, not a continuous adaptive capability. Automated rule generation might create new detections, but it doesn't inherently reduce noise unless paired with tuning.
Data integration enhancement improves coverage and correlation, but by itself it can increase alerts if not tuned. The described outcome-less noise, better precision, quicker true detection-matches adaptive tuning and optimization of detections over time, which is dynamic rule optimization.

**NEW QUESTION # 76**

Juliea a SOC analyst, while monitoring logs, noticed large TXT, NULL payloads.
What does thisindicate?

- A. Covering Tracks Attempt
- B. Concurrent VPN Connections Attempt
- C. DHCP Starvation Attempt
- D. DNS Exfiltration Attempt

**Answer: D**

Explanation:
Juliea, the SOC analyst, noticed large TXT and NULL payloads in the logs. This is indicative of a DNS exfiltration attempt. DNS exfiltration is a type of cyber attack where an attacker uses the DNS protocol to sneak data out of a network undetected. It typically involves the use of large TXT records, which can be used to carry data out of the network. NULL payloads can be used in this context to pad the DNS queries and make them less suspicious or to bypass security controls that inspect the content of DNSqueries.
The steps involved in DNS exfiltration include:
* The attacker compromises a system within the target network.
* Malware on the compromised system encodes the data it wants to exfiltrate.
* The encoded data is split into chunks that fit into DNS query sizes.
* These chunks are sent as data in DNS queries or responses, often using TXT records.
* An external attacker-controlled server receives the DNS queries and decodes the data.
References:
EC-Council's Certified SOC Analyst (CSA) course material and study guides provide detailed information on various types of cyber attacks, including DNS exfiltration.
Online resources and practice questions for the Certified SOC Analyst (CSA) exam also cover this topic and can be used to verify the answer123.
Additional information on DNS exfiltration techniques and detection methods can be found in security blogs and articles that discuss the subject in depth456.
Reference: https://www.google.com/url?
sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj8gZaKq_PuAhWGi1wKHfQTC0oQFjAAegQIAR
&url=https%3A%2F%2Fconf.splunk.com%2Fsession%2F2014%
2Fconf2014_FredWilmotSanfordOwings_Splunk_Security.pdf&usg=AOvVaw3ZLfzGqM-VUG7xKtze67ac

**NEW QUESTION # 77**
In which of the following incident handling and response stages, the root cause of the incident must be found from the forensic results?

- A. Eradication
- B. Evidence Gathering
- C. Evidence Handling
- D. SystemsRecovery

**Answer: A**

Explanation:
The eradication stage is where the root cause of the incident is determined from the forensic results. This stage involves not only removing the threat from the affected systems but also identifying and fixing the vulnerabilities that were exploited. It's crucial to understand how the incident occurred to prevent future occurrences. After the containment stage, where the immediate threat is isolated, eradication ensures that the threat is completely removed and that the root cause is addressed.
References: The EC-Council's Certified Incident Handler (E|CIH) program outlines the stages of incident handling and response, which include preparation, identification, containment, eradication, recovery, and lessons learned. Theeradication stage specifically deals with eliminating the threat and addressing the root cause based on forensic analysis. This information is covered in the E|CIH program and can be found in the official EC-Council learning resources1.
Reference: https://www.eccouncil.org/wp-content/uploads/2019/02/ECIH-V2-Brochure.pdf

**NEW QUESTION # 78**
A type of threatintelligent that find out the information about the attacker by misleading them is known as
.

- A. Counter Intelligence
- B. Detection Threat Intelligence
- C. Threat trending Intelligence
- D. Operational Intelligence

**Answer: A**

Explanation:
CounterIntelligence in the context of threat intelligence refers to efforts to deceive, manipulate, or mislead potential attackers to uncover their intentions, capabilities, or identities. This type of intelligence is proactive and often involves setting up honeypots or other traps to engage the attacker without them realizing they are being monitored and analyzed. The goal is to gather information about the attacker that can be used to strengthen defenses and prevent future attacks.
References: The EC-Council's Certified Threat Intelligence Analyst (CTIA) program discusses various types of threat intelligence, including counter intelligence, which is designed to mislead attackers and gather information about them1. This concept is also covered in the Certified SOC Analyst (CSA) training, where analysts learn to use predictive capabilities using threat intelligence to detect and counteract sophisticated threats2. Additional resources and study guides from the EC-Council and other cybersecurity training programs will provide more in-depth information on this topic34.

**NEW QUESTION # 79**
......

More and more people look forward to getting the 312-39 certification by taking an exam. However, the exam is very difficult for a lot of people. Especially if you do not choose the correct study materials and find a suitable way, it will be more difficult for you to pass the exam and get the EC-COUNCIL related certification. If you want to get the related certification in an efficient method, please choose the 312-39 learning dumps from our company. We can guarantee that the study materials from our company will help you pass the exam and get the certification in a relaxed and efficient method.

**New 312-39 Test Discount**: https://www.validexam.com/312-39-latest-dumps.html

- Free 312-39 Practice □ Reliable 312-39 Braindumps Questions □ Reliable 312-39 Practice Materials □ Easily obtain ✔ 312-39 □✔□ for free download through ⇛ www.troytecdumps.com ⇚ □Test 312-39 Result
- 312-39 Reliable Test Pdf □ 312-39 Braindumps Torrent □ Minimum 312-39 Pass Score □ Copy URL ➡ www.pdfvce.com □□□ open and search for □ 312-39 □ to download for free □312-39 Reliable Test Pdf
- Valid 312-39 Exam Camp | Pass-Sure New 312-39 Test Discount: Certified SOC Analyst (CSA) □ Easily obtain ➽ 312-39 □ for free download through ➥ www.vce4dumps.com □ □312-39 Exams Torrent
- Minimum 312-39 Pass Score □ Accurate 312-39 Prep Material □ 312-39 Latest Exam Registration □ Simply search for □ 312-39 □ for free download on ➽ www.pdfvce.com □ □312-39 Exams Torrent
- 312-39 Knowledge Points □ Exam 312-39 Practice □ Free 312-39 Practice □ Search for 《 312-39 》 and download exam materials for free through ▸ www.pass4test.com ◂ □Free 312-39 Practice
- 312-39 Latest Exam Registration □ Test 312-39 Result □ Discount 312-39 Code □ Search for （ 312-39 ） and download exam materials for free through ➡ www.pdfvce.com □□□ □312-39 Braindumps Torrent
- 312-39 Pdf Pass Leader □ 312-39 Reliable Exam Pass4sure □ Discount 312-39 Code □ Open website ▹ www.exam4labs.com ◃ and search for ⇛ 312-39 ⇚ for free download □Reliable 312-39 Practice Materials
- Reliable 312-39 Braindumps Questions □ Reliable 312-39 Test Book □ Reliable 312-39 Practice Materials □ Search on □ www.pdfvce.com □ for ➡ 312-39 □□□ to obtain exam materials for free download □312-39 Exams Torrent
- Accurate 312-39 Prep Material □ 312-39 Test Pdf □ Exam 312-39 Practice □ Search for ▸ 312-39 ◂ and download it for free immediately on ▸ www.testkingpass.com ◂ □Minimum 312-39 Pass Score
- 312-39 Reliable Exam Pass4sure □ Test 312-39 Result □ 312-39 Braindumps Torrent □ Open ➥ www.pdfvce.com □ enter ▹ 312-39 ◃ and obtain a free download □312-39 Reliable Exam Pass4sure
- 100% Pass Quiz Authoritative EC-COUNCIL - Valid 312-39 Exam Camp □ Immediately open " www.examdiscuss.com " and search for ➤ 312-39 □ to obtain a free download □Accurate 312-39 Prep Material
- 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, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, capacitacion.axiomamexico.com.mx, 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, bbs.t-firefly.com, Disposable vapes

P.S. Free 2026 EC-COUNCIL 312-39 dumps are available on Google Drive shared by ValidExam:

https://drive.google.com/open?id=1cR6JvtiW7Fex9stGcmpcEJkqD5Y9lvlg