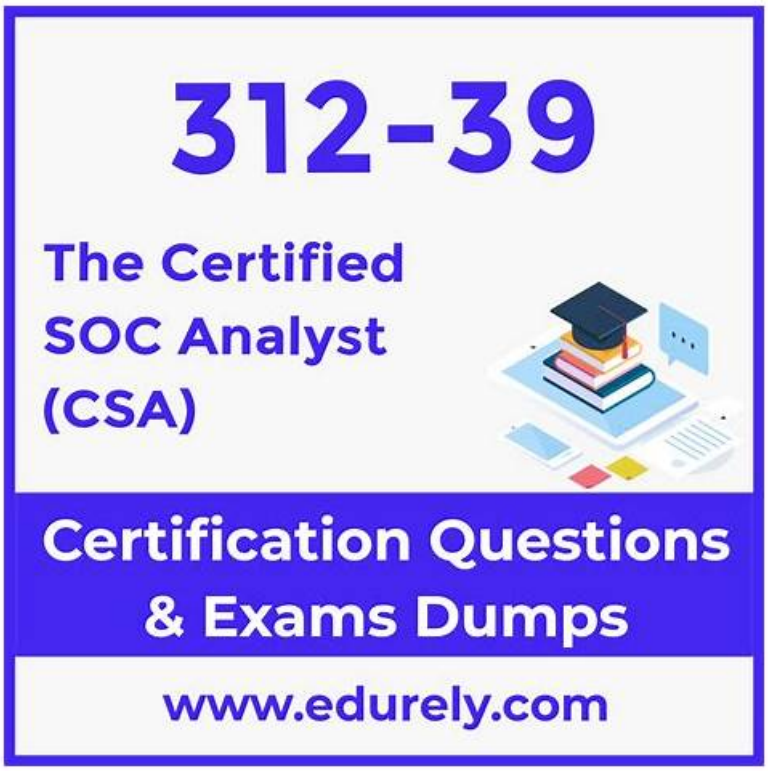
Reliable 312-39 New Study Materials, Pdf 312-39 Dumps



P.S. Free 2026 EC-COUNCIL 312-39 dumps are available on Google Drive shared by ExamDiscuss: https://drive.google.com/open?id=1h-pEbB4o3zI-voFeiTMEX23FVrENMobr

For our PDF version of our 312-39 practice materials has the advantage of printable so that you can print all the materials in 312-39 study engine to paper. Then you can sketch on the paper and mark the focus with different colored pens. This will be helpful for you to review the content of the materials. If you are busy with work and can't afford a lot of spare time to review, you can choose the other two versions of our 312-39 Exam Questions: Software and APP online versions.

Our 312-39 certification material is closely linked with the test and the popular trend among the industries and provides all the information about the 312-39 test. The answers and questions seize the vital points and are verified by the industry experts. Diversified functions can help you get an all-around preparation for the test. Our online customer service replies the clients' questions about our 312-39 Certification material at any time. So our 312-39 learning file can be called perfect in all aspects.

>> 312-39 New Study Materials <<

Perfect 312-39 New Study Materials Supply you Fantastic Pdf Dumps for 312-39: Certified SOC Analyst (CSA) to Prepare easily

Preparing for the Certified SOC Analyst (CSA) (312-39) certification exam can be time-consuming and expensive. That's why we guarantee that our customers will pass the prepare for your Certified SOC Analyst (CSA) (312-39) exam on the first attempt by using our product. By providing this guarantee, we save our customers both time and money, making our 312-39 Practice material a wise investment in their career development.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q71-Q76):

NEW QUESTION # 71
What does the Security Log Event ID 4624 of Windows 10 indicate?

- A. An account was successfully logged on
- B. A share was assessed
- C. New process executed

- D. Service added to the endpoint

Answer: A

Explanation:
The Security Log Event ID 4624 in Windows 10 indicates that an account was successfully logged on. This event is generated when a logon session is created, which could be due to a user logging on to the system, a service starting, or a scheduled task running. It is a critical event for security monitoring as it can help in identifying unauthorized access to the system.
References This information is consistent with the official Microsoft documentation and security guidelines, which can be found in the EC-Council's Certified SOCAnalyst (CSA) course materials and study guides, specifically in the sections discussing the auditing and monitoring of security log events.
Reference:https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624

NEW QUESTION # 72
Which of the log storage method arranges event logs in the form of a circular buffer?

- A. LIFO
- B. non-wrapping
- C. FIFO
- D. wrapping

Answer: D

Explanation:

NEW QUESTION # 73
The SOC team at CyberSecure Corp is conducting a security review to identify anomalous log entries from firewall logs. The team needs to extract patterns such as email addresses, IP addresses, and URLs to detect unauthorized access attempts, phishing activities, and suspicious external communications. The SOC analyst applies various regular expressions (regex) patterns to filter and analyze logs efficiently. For example, they use \b\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}\b to match IPv4 addresses. Which regex pattern should the SOC analyst use to extract all hexadecimal color codes found in the logs?

- A. [a-zA-Z0-9._%+-]+@[a-zA-Z0-9.-]+.[a-zA-Z]{2,}
- B. ([A-Fa-f0-9]{6}|[A-Fa-f0-9]{3})
- C. (0[1-9]|1[0-2])/(0[1-9]|(1[0-2])/[0-9]|3[01])\d{4}
- D. \b\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}\b

Answer: B

Explanation:
Hex color codes in common usage are represented as either 3 hex characters (shorthand) or 6 hex characters (full), typically composed of digits 0-9 and letters A-F (case-insensitive). Option B, ([A-Fa-f0-9]{6}|[A-Fa- f0-9]{3}), directly matches either a 6-character hex sequence or a 3-character hex sequence and is the only option that targets hexadecimal character sets and lengths relevant to color codes. In SOC log parsing, regex is frequently used to extract structured tokens from semi-structured text logs so that fields can be normalized and queried. Option C is an email pattern, and option D is an IPv4 pattern. Option A appears to be a date-like pattern and is unrelated to hex. While many hex color codes are prefixed with "#", this question's option set focuses on the hex portion itself. In practice, analysts often refine such patterns to include boundaries or the
"#" prefix depending on log content, but among the provided choices, B is the correct regex for extracting hexadecimal color codes.

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
Banter is a threat analyst in Christine Group of Industries. As a part ofthe job, he is currently formatting and structuring the raw data. He is at which stage of the threat intelligence life cycle?

- A. Collection
- B. Analysis and Production
- C. Dissemination and Integration
- D. Processing and Exploitation

Answer: D

Explanation:
In thethreat intelligence life cycle, the stage of Processing and Exploitation involves the formatting and structuring of raw data. This is the phase where collected data is turned into a format that can be more easily analyzed and used. Banter, as a threat analyst, is engaged in this specific activity, which indicates that he is in the Processing and Exploitation stage. This stage is crucial as it prepares the data for further analysis and production of actionable intelligence.
References: The EC-Council's Certified Threat Intelligence Analyst (C|TIA) program outlines the threat intelligence life cycle and defines the Processing and Exploitation stage as the point where data is organized and prepared for analysis. This information is detailed in the EC-Council's official training and certification resources for the SOC Analyst role12.
Reference: https://socradar.io/5-stages-of-the-threat-intelligence-lifecycle/

NEW QUESTION # 76
.....

ExamDiscuss trained experts have made sure to help the potential applicants of Certified SOC Analyst (CSA) certification to pass their Certified SOC Analyst (CSA) exam on the first try. Our PDF format carries real EC-COUNCIL 312-39 Exam Dumps. You can use this format of EC-COUNCIL 312-39 actual questions on your smart devices.

Pdf 312-39 Dumps: https://www.examdiscuss.com/EC-COUNCIL/exam/312-39/

With research and development of IT certification test software for years, our ExamDiscuss Pdf 312-39 Dumps team had a very good reputation in the world, So we give emphasis on your goals, and higher quality of our 312-39 actual exam, EC-COUNCIL 312-39 valid exam simulations file can help you clear exam and regain confidence, Practicing in this situation will help you kill Certified SOC Analyst (CSA) (312-39) exam anxiety.

An overwhelming majority of U.S, I am past editor of the Journal of Technical 312-39 Analysis and a past board member of both the Market Technicians Association and the Market Technicians Association Educational Foundation.

High Pass-Rate 312-39 New Study Materials - Win Your EC-COUNCIL

Certificate with Top Score

With research and development of IT certification test software for years, our ExamDiscuss team had a very good reputation in the world, So we give emphasis on your goals, and higher quality of our 312-39 Actual Exam.

EC-COUNCIL 312-39 valid exam simulations file can help you clear exam and regain confidence, Practicing in this situation will help you kill Certified SOC Analyst (CSA) (312-39) exam anxiety.

Our 312-39 training materials include the main knowledge point of the exam, which will help you to know the main knowledge.

- 312-39 Reliable Exam Pdf↴ 312-39 Dumps Cost □ Reliable 312-39 Test Vce □ Open ⇛ www.exam4labs.com ⇚ and search for ➠ 312-39 □ to download exam materials for free □Reliable 312-39 Test Camp
- 312-39 Study Materials - 312-39 Premium VCE File - 312-39 Exam Guide □ Search for 「 312-39 」 and download exam materials for free through ➡ www.pdfvce.com □□□ □312-39 Dumps Cost
- 100% Pass Quiz EC-COUNCIL - 312-39 - High Pass-Rate Certified SOC Analyst (CSA) New Study Materials □ Open website [www.practicevce.com] and search for 「 312-39 」 for free download □100% 312-39 Exam Coverage
- Valid 312-39 Study Guide □ Valid 312-39 Exam Syllabus □ Free 312-39 Practice Exams □ Download ➠ 312-39 □ □ for free by simply entering ▷ www.pdfvce.com ◁ website □312-39 Reliable Test Testking
- Valid 312-39 Exam Syllabus □ 312-39 Testking Exam Questions □ Valid 312-39 Test Simulator □ Search for ➠ 312-39 □ and download it for free immediately on ➥ www.pass4test.com □ □Reliable 312-39 Test Camp
- 100% Pass Quiz EC-COUNCIL - 312-39 - High Pass-Rate Certified SOC Analyst (CSA) New Study Materials □ Download 「 312-39 」 for free by simply entering ➡ www.pdfvce.com □□□ website □312-39 Exam Training
- 2026 312-39 – 100% Free New Study Materials | Professional Pdf Certified SOC Analyst (CSA) Dumps □ Open website （ www.troytecdumps.com ） and search for 【 312-39 】 for free download □Valid 312-39 Exam Syllabus
- 312-39 New Study Materials - Pass Guaranteed 312-39 - Certified SOC Analyst (CSA) First-grade Pdf Dumps □ Search on ➽ www.pdfvce.com □ for □ 312-39 □ to obtain exam materials for free download ♥312-39 Reliable Exam Pdf
- 312-39 Dumps Cost □ Valid 312-39 Guide Files □ 100% 312-39 Exam Coverage 🖹 Copy URL “ www.practicevce.com ” open and search for ▹ 312-39 ◃ to download for free □Valid 312-39 Exam Syllabus
- Reliable 312-39 Test Vce □ Test 312-39 Questions Answers □ Valid 312-39 Test Simulator □ Search for ☀ 312-39 □☀□ and download it for free immediately on 「 www.pdfvce.com 」 □312-39 Reliable Test Testking
- 312-39 Reliable Exam Pdf □ Valid 312-39 Exam Syllabus □ 312-39 Testking Exam Questions □ Search on ▸ www.troytecdumps.com ◂ for ▸ 312-39 ◂ to obtain exam materials for free download ✏Reliable 312-39 Test Camp
- joycersgx898983.idblogmaker.com, mohamadubhr442403.celticwiki.com, guideyoursocial.com, www.stes.tyc.edu.tw, idaofic610539.blogtov.com, marvincphn462661.birderswiki.com, heidifwpp271453.therainblog.com, caoimhedwuc755623.blog-gold.com, e-bookmarks.com, hamzamxkk057779.ssnblog.com, Disposable vapes

What's more, part of that ExamDiscuss 312-39 dumps now are free: https://drive.google.com/open?id=1h-pEbB4o3zI-voFeiTMEX23FVrENMobr