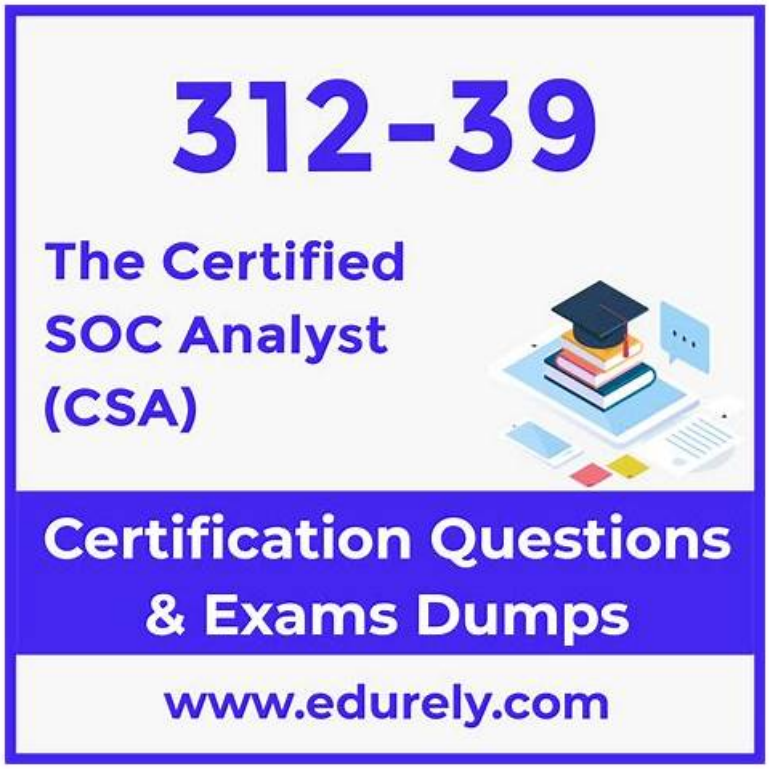
Free PDF 312-39 Free Exam Dumps–Authorized Reliable Test Notes for 312-39



BTW, DOWNLOAD part of PrepPDF 312-39 dumps from Cloud Storage: https://drive.google.com/open?id=1svVi3uJOfeg0Y7SJj9r4dasLdyigELeh

By using our 312-39 study engine, your abilities will improve and your mindset will change. Who does not want to be a positive person? This is all supported by strength! In any case, a lot of people have improved their strength through 312-39 Exam simulating. They now have the opportunity they want. Whether to join the camp of the successful ones, purchase 312-39 learning braindumps, you decide for yourself!

The Certified SOC Analyst (CSA) certification exam is designed for professionals who want to advance their security careers and stay ahead of the curve in this fast-paced industry. It is especially appropriate for those who work in security operations centers or want to improve their knowledge in this area. The CSA certification exam covers a wide range of topics, including threat intelligence, incident response, network security, and log analysis, among others. Professionals who pass the exam show they have the knowledge and analytical skills needed to handle complex cybersecurity threats.

>> 312-39 Free Exam Dumps <<

Reliable 312-39 Test Notes & 312-39 Exam Engine

As is known to all, before purchasing the 312-39 Study Guide, we need to know the features of it. We offer you free demo to have a try, so that you can know the characteristics of 312-39 exam dumps. Beside we have three versions, each version have its own advantages, and they can meet all of your demands. And we have free update for 365 days after buying, the latest version will send to you email box automatically.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q195-Q200):

NEW QUESTION # 195
Which of the following formula represents the risk levels?

- A. Level of risk = Consequence × Asset Value

- B. Level of risk = Consequence × Likelihood
- C. Level of risk = Consequence × Impact
- D. Level of risk = Consequence × Severity

Answer: B

Explanation:
The level of risk is typically calculated by considering the consequence (or impact) of an event and the likelihood (or probability) of its occurrence. The formula represents a fundamental risk assessment concept where risk is the product of the two factors:
* Consequence (Impact): The outcome or result if a threat does exploit a vulnerability.
* Likelihood (Probability): The chance that a given threat will exploit a vulnerability.
By multiplying these two factors, one can determine the level of risk, which helps in prioritizing risks and deciding on the appropriate level of controls and mitigation strategies.
References: The EC-Council's Certified SOC Analyst (CSA) course materials and study guides cover the concepts of risk assessment and management, which include the formula for calculating risk levels as the product of consequence and likelihood. These concepts are aligned with industry best practices and standards for security operations centers.

NEW QUESTION # 196
Which of the log storage method arranges event logs in the form of a circular buffer?

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

Answer: B

NEW QUESTION # 197
Which of the following command is used to enable logging in iptables?

- A. $ iptables -A OUTPUT -j LOG
- B. $ iptables -A INPUT -j LOG
- C. $ iptables -B OUTPUT -j LOG
- D. $ iptables -B INPUT -j LOG

Answer: B

Explanation:

NEW QUESTION # 198
Which of the following command is used to enable logging in iptables?

- A. $ iptables -A INPUT -j LOG
- B. $ iptables -B OUTPUT -j LOG
- C. $ iptables -A OUTPUT -j LOG
- D. $ iptables -B INPUT -j LOG

Answer: C

NEW QUESTION # 199
Which of the following threat intelligence is used by a SIEM for supplying the analysts with context and "situational awareness" by using threat actor TTPs, malwarecampaigns, tools used by threat actors.
1.Strategic threat intelligence
2.Tactical threat intelligence
3.Operational threat intelligence
4.Technical threat intelligence

- A. 2 and 3
- B. 1 and 2
- C. 3 and 4
- D. 1 and 3

Answer: A

Explanation:
Reference:https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A- Guide-For-Decision-Makers-and-Analysts-v2.0.pdf (38)

NEW QUESTION # 200
.....

A considerable amount of effort goes into our products. So in most cases our 312-39 exam study materials are truly your best friend. On one hand, our 312-39 learning guide is the combination of the latest knowledge and the newest technology, which could constantly inspire your interest of study. On the other hand, our 312-39 test answers can predicate the exam correctly. Therefore you can handle the questions in the real exam like a cork. Through highly effective learning method and easily understanding explanation, you will pass the 312-39 Exam with no difficulty. Our slogans are genuinely engraving on our mind that is to help you pass the 312-39 exam, and ride on the crest of success!

BTW, DOWNLOAD part of PrepPDF 312-39 dumps from Cloud Storage: https://drive.google.com/open?id=1svVi3uJOfeg0Y7SJj9r4dasLdyigELeh