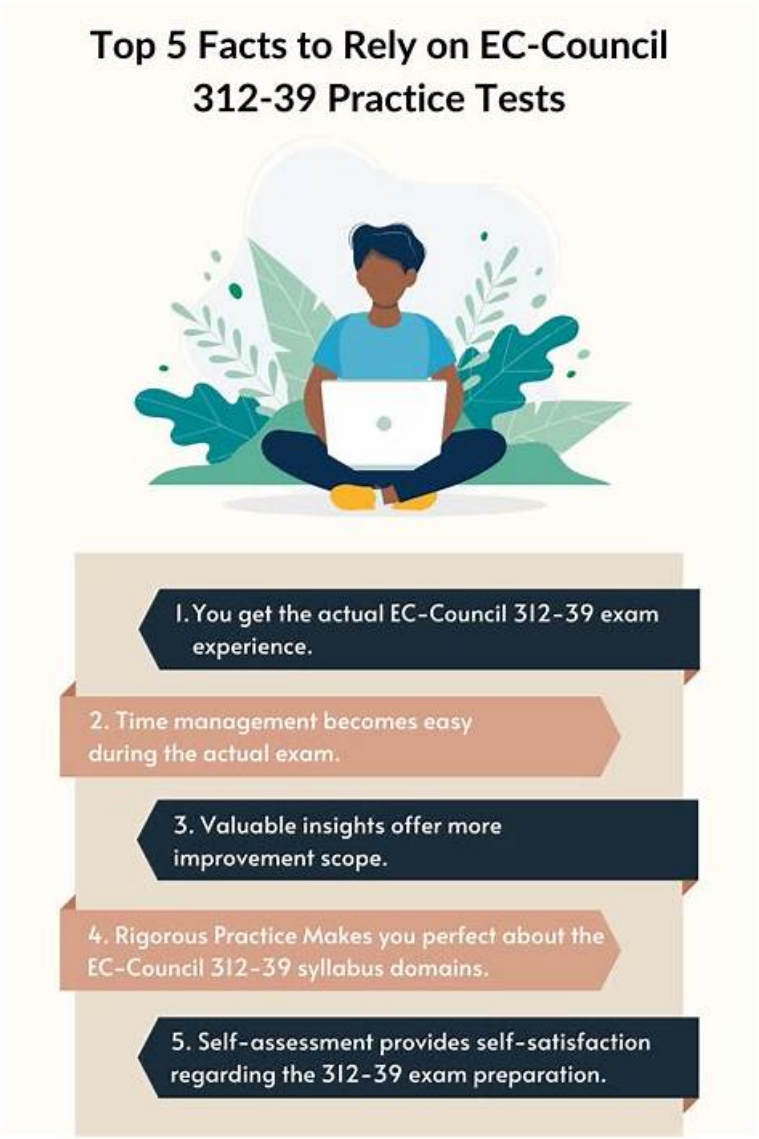
Quiz EC-COUNCIL - Useful 312-39 Exam Topics



BONUS!!! Download part of TorrentValid 312-39 dumps for free: https://drive.google.com/open?id=1QZ6ryHH5AwO0Vji3zI0nY0RpQhrzqQw4

312-39 test questions have a mock examination system with a timing function, which provides you with the same examination environment as the real exam. Although some of the hard copy materials contain mock examination papers, they do not have the automatic timekeeping system. Therefore, it is difficult for them to bring the students into a real test state. With 312-39 Exam Guide, you can perform the same computer operations as the real exam, completely taking you into the state of the actual exam, which will help you to predict the problems that may occur during the exam, and let you familiarize yourself with the exam operation in advance and avoid rushing during exams.

The CSA certification exam covers a wide range of topics related to security operations, including incident response, threat intelligence, network security, endpoint security, and security analytics. 312-39 exam consists of 100 multiple-choice questions and is designed to test the learner's knowledge and expertise in the field of security operations. 312-39 Exam is conducted online and can be taken from anywhere in the world, making it a convenient option for busy professionals.

>> 312-39 Exam Topics <<

312-39 test braindumps: Certified SOC Analyst (CSA) - 312-39 test-king

guide & 312-39 test torrent

Do you often feel that your ability does not match your ambition? Are you dissatisfied with the ordinary and boring position? If your answer is yes, you can try to get the 312-39 certification that you will find there are so many chances wait for you. You can get a better job; you can get more salary. But if you are trouble with the difficult of 312-39 Exam, you can consider choose 312-39 guide question to improve your knowledge to pass 312-39 exam, which is your testimony of competence. We believe our latest 312-39 exam torrent will be the best choice for you.

The CSA certification is designed to equip professionals with the knowledge and skills required to effectively handle security incidents, manage risk, and implement effective security measures. Certified SOC Analyst (CSA) certification covers a wide range of topics, including threat intelligence, incident response, network security, and risk management. It is an advanced certification that requires candidates to have prior experience in the field of cybersecurity.

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

NEW QUESTION # 74
David is a SOC analyst responsible for monitoring critical infrastructure. He detects unauthorized applications running on a high-privilege Windows server accessible only by a restricted set of users. The applications were not part of approved deployments, and installations occurred outside business hours. Logs indicate potential system configuration changes around the same timeframe.
Which log should he examine to determine when and how these installations occurred?

- A. Security event log
- B. Application event log
- C. System event log
- D. Setup event log

Answer: D

Explanation:
The Setup event log is the most relevant Windows log for installation activity because it captures events related to software installation, servicing, and setup operations. For unauthorized application installs, the SOC needs timing, installer context, and evidence of package deployment or configuration changes driven by setup processes. The Setup log can contain MSI and update-related events, component installation records, and indications of system changes tied to installation workflows. The Security log is crucial for attribution (logons, privilege use, process creation if enabled), but it is not specifically focused on installer actions and may not capture full installation details unless advanced auditing is configured. The System log focuses on OS-level service and driver events (boot, service start/stop, hardware/driver issues) and may show related changes but is not the primary installation record. The Application log captures events written by applications themselves, which is inconsistent for installer tracing. In SOC practice, analysts often combine Setup log evidence with Security log context (who logged on, elevated rights, process lineage) and endpoint telemetry to identify the actor and technique, but the best single log for "when and how installs occurred" among these options is the Setup event log.

NEW QUESTION # 75
Which of the following framework describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering?

- A. COBIT
- B. SSE-CMM
- C. SOC-CMM
- D. ITIL

Answer: B

NEW QUESTION # 76
An organization is implementing and deploying the SIEM with following capabilities.
What kind of SIEM deployment architecture the organization is planning to implement?

- A. Cloud, MSSP Managed
- B. Self-hosted, Jointly Managed

- C. Self-hosted, MSSP Managed
- D. Self-hosted, Self-Managed

Answer: D

Explanation:

NEW QUESTION # 77
Which of the following command is used to enable logging in iptables?

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

Answer: B

NEW QUESTION # 78
A SOC analyst receives an alert indicating that the system time on a critical Windows server was changed at 3:
00 AM. There are no scheduled maintenance tasks at this time. Unauthorized time changes can be used to evade security controls, such as altering timestamps to obscure malicious activity. The analyst must identify the relevant event codes that log system time modifications and related suspicious behavior. Which of the following Windows Security Event Codes should the analyst review to investigate potential tampering?

- A. 4616 and 4624
- B. 4616 and 4618
- C. 4608 and 4609
- D. 4625 and 4634

Answer: B

Explanation:
Event ID 4616 is the key Windows Security log event for "system time was changed," and it is the primary artifact to confirm and investigate time-tampering. It typically includes details such as the previous time, the new time, and the account or process context responsible, which helps the SOC determine whether the change was authorized (maintenance) or suspicious (off-hours, unusual account, unexpected host). Event ID 4618 is useful as a companion signal because it indicates monitored security-relevant conditions and can help reveal related suspicious behavior around auditing or security event patterns that may coincide with timestamp manipulation. In practice, SOC analysts correlate the time-change event with surrounding authentication events, privilege use, and process creation telemetry to identify the actor and intent. The other options do not directly target the time-change activity:
4608/4609 relate to system startup/shutdown; 4625 is failed logon and
4634 is logoff; 4624 is successful logon (useful context, but not the event that records the time modification itself). Therefore, the best pairing for investigating time tampering in the options provided is 4616 and 4618.

NEW QUESTION # 79
.....

- Reliable and Guarantee Refund of EC-COUNCIL 312-39 Exam Questions □ Search on ▷ www.pdfvce.com ◁ for ✔ 312-39 □✔□ to obtain exam materials for free download □312-39 Test Pdf
- Use EC-COUNCIL 312-39 Practice Exam Software (Desktop and Web-Based) For Self Evaluation □ Enter ➡ www.easy4engine.com □□□ and search for □ 312-39 □ to download for free □312-39 Latest Study Plan
- 312-39 Valid Exam Tutorial □ Answers 312-39 Free □ New 312-39 Test Topics □ Enter ☀ www.pdfvce.com □☀□ and search for 「 312-39 」 to download for free □Reliable 312-39 Test Tips
- First-rank 312-39 Practice Materials Stand for Perfect Exam Dumps - www.testkingpass.com □ Search for ⇛ 312-39 ⇚ and download it for free on ➡ www.testkingpass.com □□□ website □312-39 Test Pdf
- 312-39 - Certified SOC Analyst (CSA) Perfect Exam Topics □ Simply search for ➡ 312-39 □□□ for free download on ▷ www.pdfvce.com ◁ □Reliable 312-39 Test Tips
- Reliable and Guarantee Refund of EC-COUNCIL 312-39 Exam Questions □ Search on ▷ www.exam4labs.com ◁ for " 312-39 " to obtain exam materials for free download □Reliable 312-39 Exam Simulations
- myportal.utt.edu.tt, portfolium.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, Disposable vapes

P.S. Free & New 312-39 dumps are available on Google Drive shared by TorrentValid: https://drive.google.com/open?id=1QZ6ryHH5AwO0Vji3zI0nY0RpQhrzqQw4