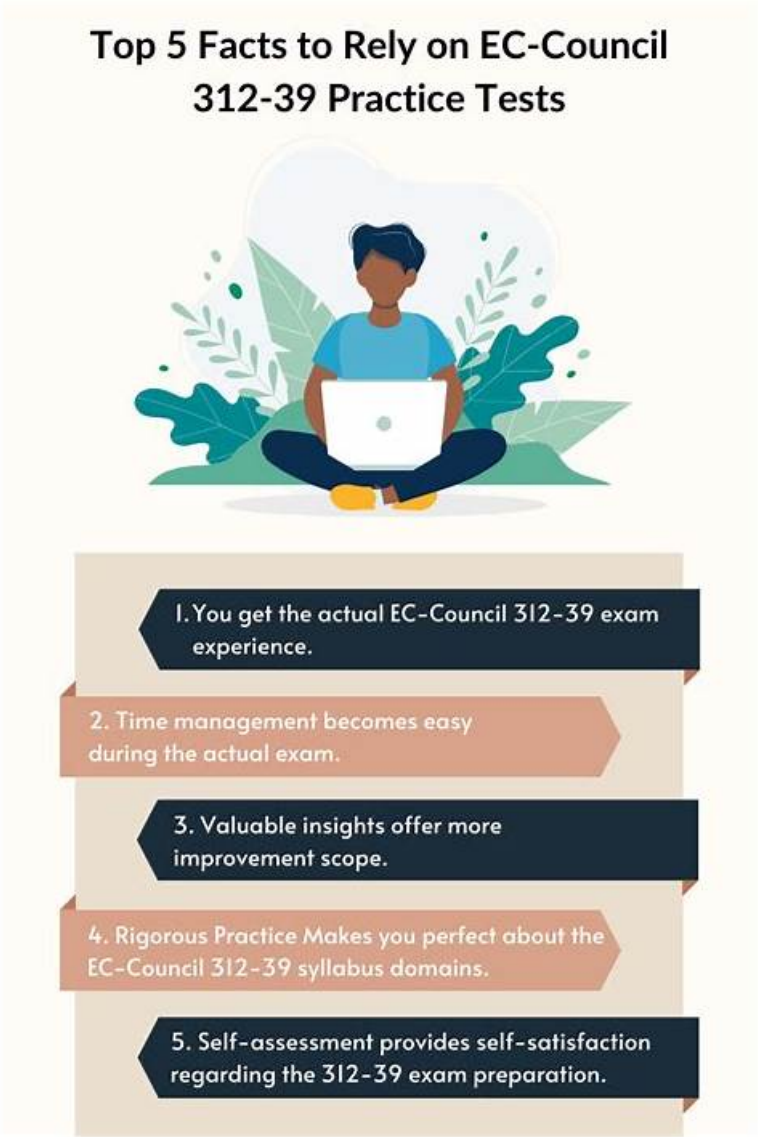
312-39 PDF Questions [2026]-Right Preparation Material



P.S. Free & New 312-39 dumps are available on Google Drive shared by TroytecDumps: https://drive.google.com/open?id=1DnKDuLdXhobCJid0c-gL2oDo4zFjg56f

As is known to all, for the candidates who will attend the exam, knowing the latest version is quite significant. Our 312-39 training materials are free update for 365 days after purchasing. And the updated version will be sent to your email address automatically by our system. Besides, our 312-39 Training Materials are verified by the skilled professionals, and the accuracy and the quality can be guaranteed. By using the 312-39 exam dumps of us, you can also improve your efficiency, since it also has knowledge points.

The Certified SOC Analyst (CSA) certification exam is based on the EC-Council's CSA course, which covers a wide range of topics related to SOC operations. 312-39 course is designed to provide candidates with a comprehensive understanding of the tools, techniques, and processes used in SOC operations. Candidates who successfully pass the exam will be able to demonstrate their ability to identify security incidents, analyze security logs, and respond to security incidents in a timely and effective manner.

>> 312-39 Cert Guide <<

EC-COUNCIL 312-39 Guaranteed Success - 312-39 Free Practice

There is an irreplaceable trend that an increasingly amount of clients are picking up 312-39 study materials from tremendous practice materials in the market. There are unconquerable obstacles ahead of us if you get help from our 312-39 Exam Questions. So many

exam candidates feel privileged to have our 312-39 practice braindumps. And our website is truly very famous for the hot hit in the market and easy to be found on the internet.

The EC-Council 312-39 Exam marks the initial step to becoming an important part of a Security Operations Center (SOC). It is a qualification test for the Certified SOC Analyst (CSA) certification and restructured to suit SOC analysts across the two popular tiers (Tier I & Tier II). All in all, this test will help you perform better and achieve more in entry and mid-level job roles as far as SOC teams are involved. In particular, the following groups may benefit from this training:

- SOC analysts;
- Baseline-level cybersecurity specialists;
- Any individual looking to become a SOC analyst.
- Cybersecurity analysts;

EC-COUNCIL's Certified SOC Analyst (CSA) Exam is an essential certification for anyone interested in establishing a career in the cybersecurity field. With the right study materials and a dedication to learning, passing the CSA exam can prepare you for an exciting career in Security Operations Center (SOC), incident response, and many more cybersecurity areas. The CSA exam is an essential first step to building a successful career in cybersecurity.

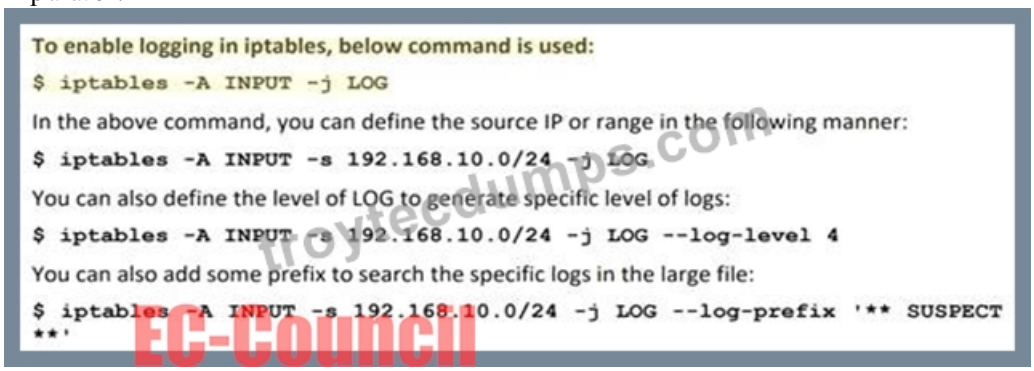
EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q183-Q188):

NEW QUESTION # 183
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 # 184
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. True Positive Incidents
- B. True Negative Incidents
- C. False positive Incidents
- D. False Negative Incidents

Answer: D

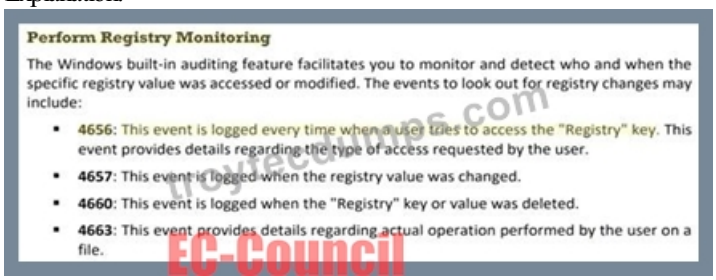
Explanation:
A false negative incident in the context of a Security Operations Center (SOC) is when an actual attack or intrusion occurs, but the SOC analyst fails to detect any suspicious events or indicators of compromise. This means that the security measures in place did not work as intended, and 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 # 185
Which of the following Windows event is logged every time when a user tries to access the "Registry" key?

- A. 0
- B. 1
- C. 2
- D. 3

Answer: D

Explanation:



NEW QUESTION # 186
A threat hunter analyzing an infected endpoint finds that malicious processes keep reappearing even after termination, making traditional remediation ineffective. The user reports slowdowns, abnormal pop-ups, and unauthorized application launches. Deeper inspection reveals multiple scheduled tasks executing unknown scripts at intervals, along with suspicious registry modifications enabling automatic execution on startup. The endpoint makes intermittent encrypted outbound connections to an unclassified external server. The organization also observed multiple failed privileged logins from the same subnet. Which signs should the threat hunter look for to confirm and mitigate the threat?

- A. Threat intelligence and adversary context
- B. Indicators of Attack (IoAs)
- C. Host-based artifacts
- D. Network-based artifacts

Answer: C

Explanation:
Host-based artifacts are the most direct evidence to confirm persistence and recurring execution on an endpoint. The scenario already describes classic host persistence mechanisms: scheduled tasks and registry autorun modifications. To confirm and mitigate, a threat hunter should focus on endpoint-resident artifacts such as: persistence entries (scheduled tasks, Run/RunOnce keys, services, WMI subscriptions), process ancestry (which parent launches the malicious script), file system changes (dropped scripts, DLLs, staged payloads), and security control tampering. These artifacts enable containment and eradication because they point to what must be removed and what must be prevented from re-creating itself after reboot. Network- based artifacts are important for identifying C2 destinations and potential lateral movement, but they won't fully explain how the malware survives termination. Threat intelligence context can help attribute and match TTPs, but it's not required to confirm persistence locally. Indicators of Attack are behavior patterns (like scheduled task creation, registry autoruns, process injection) and are valuable conceptually, but the option that best represents the concrete evidence you need to examine and remediate on the endpoint is "host-based artifacts." In SOC response, you'd combine host artifact removal with credential resets and scoping for similar persistence across endpoints.

NEW QUESTION # 187
Identify the event severity level in Windows logs for the events that are not necessarily significant, but may indicate a possible future problem.

- A. Error
- B. Information
- C. Warning
- D. Failure Audit

Answer: C

NEW QUESTION # 188
.....

312-39 Guaranteed Success: https://www.troytecdumps.com/312-39-troytec-exam-dumps.html

- PassLeader 312-39 Practice Materials: Certified SOC Analyst (CSA) are a wise choice - www.troytecdumps.com □ Search for 【 312-39 】 and download exam materials for free through 「 www.troytecdumps.com 」 □312-39 Free Exam Questions
- Free PDF 2026 The Best EC-COUNCIL 312-39: Certified SOC Analyst (CSA) Cert Guide □ ✔ www.pdfvce.com □✔□ is best website to obtain □ 312-39 □ for free download □312-39 Free Exam Questions
- PassLeader 312-39 Practice Materials: Certified SOC Analyst (CSA) are a wise choice - www.examcollectionpass.com □ □ Search for [312-39] and obtain a free download on ➽ www.examcollectionpass.com □ □312-39 Lab Questions
- EC-COUNCIL - Marvelous 312-39 - Certified SOC Analyst (CSA) Cert Guide □ Search for [312-39] and download it for free immediately on □ www.pdfvce.com □ □312-39 Test Vce Free
- 312-39 Cert Guide - EC-COUNCIL 312-39 Guaranteed Success: Certified SOC Analyst (CSA) Pass Certify □ Go to website ⇛ www.prep4away.com ⇚ open and search for □ 312-39 □ to download for free □Latest 312-39 Material
- 312-39 Test Collection Pdf □ 312-39 Lab Questions □ Real 312-39 Braindumps □ Copy URL [www.pdfvce.com] open and search for 「 312-39 」 to download for free □Dump 312-39 Collection
- PassLeader 312-39 Practice Materials: Certified SOC Analyst (CSA) are a wise choice - www.practicevce.com □ Open □ www.practicevce.com □ enter ✔ 312-39 □✔□ and obtain a free download ☢312-39 Pass Guaranteed
- Free PDF 2026 The Best EC-COUNCIL 312-39: Certified SOC Analyst (CSA) Cert Guide □ Easily obtain □ 312-39 □ for free download through 「 www.pdfvce.com 」 □Exam 312-39 Pass4sure
- 312-39 New Braindumps Book □ 312-39 Pass Guaranteed □ 312-39 New Braindumps Book □ The page for free download of ▸ 312-39 ◂ on ➥ www.troytecdumps.com □ will open immediately □312-39 Free Exam Questions
- Latest 312-39 Material □ 312-39 New Braindumps Free □ Latest 312-39 Questions □ Copy URL □ www.pdfvce.com □ open and search for [312-39] to download for free □Dump 312-39 Collection
- 312-39 New Braindumps Book □ 312-39 Free Sample Questions □ 312-39 Test Collection Pdf □ Go to website ➡ www.pdfdumps.com □□□ open and search for ➥ 312-39 □ to download for free □Latest 312-39 Material
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, socialaffluent.com, steveuipu299784.ourabilitywiki.com, finnianiwtm942287.dgbloggers.com, gretafpci514368.smblogsites.com, susanwvhl768572.life3dblog.com, englishsphereonline.com, mohamadfvvb460152.blogtov.com, cyruskwhp625387.fliplife-wiki.com, Disposable vapes

P.S. Free & New 312-39 dumps are available on Google Drive shared by TroytecDumps: https://drive.google.com/open?id=1DnKDuLdXhobCJid0c-gL2oDo4zFjg56f