Quiz High-quality EC-COUNCIL - Latest 312-39 Test Practice

Top 5 Facts to Rely on EC-Council 312-39 Practice Tests

1. You get the actual EC-Council 312-39 exam experience.

2. Time management becomes easy during the actual exam.

3. Valuable insights offer more improvement scope.

4. Rigorous Practice Makes you perfect about the EC-Council 312-39 syllabus domains.

5. Self-assessment provides self-satisfaction regarding the 312-39 exam preparation.

2026 Latest TorrentExam 312-39 PDF Dumps and 312-39 Exam Engine Free Share: https://drive.google.com/open?id=1wsNaAi7kmAdA6-GqGZC1kv1dQgLLV_B1

Up to now, we have business connection with tens of thousands of exam candidates who adore the quality of them. Besides, we try to keep our services brief, specific and courteous with reasonable prices of 312-39 practice materials. All your questions will be treated and answered fully and promptly. We guarantee that you can pass the exam at one time even within one week based on practicing our 312-39 studying materials regularly. 98 to 100 percent of former exam candidates have achieved their success by them.

EC-COUNCIL 312-39 (Certified SOC Analyst (CSA)) Exam is a certification exam that validates the candidate's expertise in SOC analysis. 312-39 exam covers various topics related to network security and provides the necessary skills and knowledge to become a successful SOC Analyst. Certified SOC Analyst (CSA) certification is recognized globally and highly valued by employers in the IT industry, providing a competitive edge to candidates in the job market.

>> Latest 312-39 Test Practice <<

Latest 312-39 Demo, Exam 312-39 Topic

What are you waiting for? Opportunity knocks but once. You can get EC-COUNCIL 312-39 complete as long as you enter TorrentExam website. You find the best 312-39 Exam Training materials, with our exam questions and answers, you will pass the exam.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q160-Q165):

NEW QUESTION # 160
Which of the following Windows features is used to enable Security Auditing in Windows?

- A. Windows Defender
- B. Windows Firewall
- C. Local Group Policy Editor
- D. Bitlocker

Answer: C

Explanation:
To enable Security Auditing in Windows, the Local Group Policy Editor is used. This feature allows administrators to configure security policies and audit settings on a local computer. Here's how you can enableSecurity Auditing using the Local Group Policy Editor:
* Press Win + R, type gpedit.msc, and press Enter to open the Local Group Policy Editor.
* Navigate to Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -
> Audit Policy.
* Here, you will find a list of audit policies that you can configure for both success and failure events.
* By enabling these policies, you can specify which security-related events you want to audit, such as account logon events, object access, policy change, privilege use, and more.
References: The process described above is aligned with the best practices and guidelines provided by Microsoft and other authoritative sources on Windows security auditing, such as:
Microsoft's official documentation on Security Auditing1.
Guides on how to enable Security Auditing in Active Directory environments2.
Articles detailing the essentials of Windows event log security auditing3. These references are part of the learning resources for the EC-Council SOC Analyst course and provide comprehensive information on the subject.
Reference: https://resources.infosecinstitute.com/topic/how-to-audit-windows-10-application-logs/

NEW QUESTION # 161
The threat intelligence, which will help you, understand adversary intent and make informed decision to ensure appropriate security in alignment with risk.
What kind of threat intelligence described above?

- A. Strategic Threat Intelligence
- B. Functional Threat Intelligence
- C. Tactical Threat Intelligence
- D. Operational Threat Intelligence

Answer: A

Explanation:
The type of threat intelligence that helps in understanding adversary intent and making informed decisions to ensure appropriate security in alignment with risk is known as Strategic Threat Intelligence. This form of intelligence is concerned with the broader goals and motivations of threat actors, as well as the long-term trends and implications of their activities. It provides insights into the cyber threat landscape and helps organizations shape their security strategy and policies to mitigate risks.
Strategic Threat Intelligence is used to inform decision-makers about the nature of threats, the potential impact on the organization, and the necessary steps to align security measures with business objectives. It is less technical than Tactical or Operational Threat Intelligence and does not focus on the specific details of attacks or the technical indicators of compromise. Instead, it provides a high-level view of the threats and their relevance to the organization's risk management.
References: The information provided aligns with the EC-Council's Certified Threat Intelligence Analyst (C|TIA) program, which covers the use of threat intelligence in SOC operations and the integration of threat intelligence into risk management processes1.
Additionally, the distinction between different types of threat intelligence, such as Tactical, Strategic, and Operational, is well-documented in the cybersecurity community and can be found in various threat intelligence resources23.
Reference: https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/threat- intelligence/what-is-threat-

intelligence/

NEW QUESTION # 162
You are a Threat Hunter in an IT company's security team working to enhance threat hunting capabilities.
You observed that relying solely on traditional security alerts often results in missed detections of sophisticated threats. To strengthen your approach, you decide to incorporate multiple data sources, including external threat intelligence feeds, internal security logs, network traffic data, and endpoint telemetry. To efficiently process this vast amount of data, you implement a new tool that can aggregate, normalize, and correlate threat intelligence with internal telemetry to gain a more holistic understanding of emerging threats and enhance detection accuracy. What key threat detection capability is being leveraged in this scenario?

- A. Intelligence Buy-In
- B. Data Integration
- C. Threat Trending
- D. Threat Reports

Answer: B

Explanation:
This scenario is centered on combining multiple heterogeneous data sources into a single analytical view so that signals can be correlated into higher-confidence detections. That is the core of data integration: ingesting external intelligence (malicious IPs/domains/hashes/TTPs) and internal telemetry (endpoint events, authentication, network flows, DNS, proxy, cloud logs), then normalizing and correlating them to detect activity that would be missed if each source were analyzed in isolation. In threat hunting, integration enables pivoting and validation: an external indicator becomes meaningful when matched to internal events, and internal anomalies become higher priority when they align with known adversary behaviors. "Threat reports" are outputs, not the underlying capability. "Intelligence buy-in" is governance and stakeholder support, not a technical detection capability. "Threat trending" focuses on patterns over time (frequency, prevalence), which can inform strategy but does not directly describe the aggregation/normalization/correlation capability emphasized here. For SOC analysts, data integration is what allows efficient triage and hunting at scale, reduces blind spots, and improves detection fidelity by cross-validating evidence across endpoints, identity, network, and external intelligence.

NEW QUESTION # 163
What type of event is recorded when an application driver loads successfully in Windows?

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

Answer: D

NEW QUESTION # 164
A major financial institution has strict policies preventing unauthorized data transfers. As a SOC analyst, during routine log analysis you detect an anomaly: an employee workstation initiates large file transfers outside business hours, involving highly sensitive customer financial records. You discover remote access from an unfamiliar IP address and an unauthorized USB device connection on the workstation. Given the likelihood of data exfiltration, what should be your first step in responding?

- A. Inform the employee's department and wait for evidence
- B. Disable the corporate VPN entirely
- C. Isolate the employee's workstation and revoke remote access
- D. Conduct a full forensic analysis first

Answer: C

Explanation:
The first step should prioritize immediate containment to stop ongoing exfiltration and prevent further compromise. Isolating the workstation (network isolation or EDR containment) and revoking remote access (terminate sessions, block the suspicious IP, disable the user's remote access methods) directly reduces the attacker's ability to continue transferring sensitive data and limits lateral movement risk. In incident response, containment precedes deep forensics when active harm is likely; you preserve evidence

while stopping the bleeding. Conducting full forensics first can delay containment and allow continued data theft. Disabling corporate VPN entirely is overly disruptive and does not target the specific compromised endpoint or account; it can also hinder business operations and incident response activity. Informing the department and waiting is inappropriate given the indicators of compromise and policy violation (unauthorized USB). After containment, the SOC should preserve volatile evidence if possible (RAM, active connections), collect relevant logs, assess data accessed, and coordinate with legal/HR due to insider threat implications. But the initial, highest-priority action is targeted containment of the affected workstation and access paths.

NEW QUESTION # 165

......

Our 312-39 test guides have a higher standard of practice and are rich in content. If you are anxious about how to get 312-39 certification, considering purchasing our 312-39 study tool is a wise choice and you will not feel regretted. Our learning materials will successfully promote your acquisition of certification. Our 312-39 qualification test closely follow changes in the exam outline and practice. In order to provide effective help to customers, on the one hand, the problems of our 312-39 test guides are designed fitting to the latest and basic knowledge. For difficult knowledge, we will use examples and chart to help you learn better. On the other hand, our 312-39 test guides also focus on key knowledge and points that are difficult to understand to help customers better absorb knowledge. Only when you personally experience our 312-39 qualification test can you better feel the benefits of our products. Join us soon.

Latest 312-39 Demo: https://www.torrentexam.com/312-39-exam-latest-torrent.html

- Efficient Latest 312-39 Test Practice | 100% Free Latest 312-39 Demo □ Open website ⇛ www.prepawaypdf.com ⇚ and search for ⇛ 312-39 ⇚ for free download □312-39 Exam Questions
- High Quality 312-39 Cram Training Materials Make Certified SOC Analyst (CSA) Easily □ Search for ➡ 312-39 □□□ and download exam materials for free through ✔ www.pdfvce.com □✔□ □Latest 312-39 Test Camp
- Latest Latest 312-39 Test Practice - 100% Pass 312-39 Exam □ Search for ➡ 312-39 □□□ and download it for free on （ www.pdfdumps.com ） website □Reliable 312-39 Exam Voucher
- New 312-39 Test Dumps □ Latest 312-39 Test Camp □ 312-39 Valid Exam Cost □ Go to website { www.pdfvce.com } open and search for ⇛ 312-39 ⇚ to download for free □New 312-39 Test Dumps
- 312-39 Guaranteed Questions Answers □ 312-39 Updated Testkings □ 312-39 Online Exam □ Search for { 312-39 } on □ www.examcollectionpass.com □ immediately to obtain a free download □Exam 312-39 Topics
- Free PDF Quiz High-quality EC-COUNCIL - 312-39 - Latest Certified SOC Analyst (CSA) Test Practice □ Copy URL { www.pdfvce.com } open and search for ▹ 312-39 ◃ to download for free □Test 312-39 Dates
- 312-39 – 100% Free Latest Test Practice | High-quality Latest Certified SOC Analyst (CSA) Demo □ Search for ➡ 312-39 □□□ and download it for free immediately on ☀ www.examdiscuss.com □☀□ □New 312-39 Test Dumps
- Latest Latest 312-39 Test Practice - 100% Pass 312-39 Exam □ Search for { 312-39 } and easily obtain a free download on □ www.pdfvce.com □ □Reliable 312-39 Exam Voucher
- Latest 312-39 Test Camp □ Test 312-39 Dates □ Reliable 312-39 Exam Voucher ✈ Search for □ 312-39 □ and download exam materials for free through 「 www.vce4dumps.com 」 ☑312-39 Guaranteed Questions Answers
- Free PDF Quiz High-quality EC-COUNCIL - 312-39 - Latest Certified SOC Analyst (CSA) Test Practice □ Search for （ 312-39 ） and download exam materials for free through （ www.pdfvce.com ） □Test 312-39 Dates
- Reliable 312-39 Exam Voucher □ 312-39 Guide Torrent □ 312-39 Reliable Guide Files □ Search for □ 312-39 □ and download it for free immediately on ✔ www.troytecdumps.com □✔□ □Latest 312-39 Test Camp
- 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, dataclick.in, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, academy.cooplus.org, Disposable vapes

BTW, DOWNLOAD part of TorrentExam 312-39 dumps from Cloud Storage: https://drive.google.com/open?id=1wsNaAi7kmAdA6-GqGZC1kv1dQgLLV_B1