2026 High-quality 100% Free 312-39–100% Free PDF Cram Exam | Test 312-39 Simulator Online

P.S. Free & New 312-39 dumps are available on Google Drive shared by Exam4PDF: https://drive.google.com/open?id=16JocCzWOdsBaJUKqGVlabQvuCWjMmN8r

Once you enter into our interface, nothing will disturb your learning the 312-39 training engine except the questions and answers. So all you attention will be concentrated on study. At the same time, each process is easy for you to understand. There will have small buttons on the 312-39 Exam simulation to help you switch between the different pages. It does not matter whether you can operate the computers well. Our 312-39 training engine will never make you confused.

It is a matter of common sense that pass rate of a kind of 312-39 exam torrent is the only standard to testify weather it is effective and useful. I believe that you already have a general idea about the advantages of our 312-39 exam question, but now I would like to show you the greatest strength of our 312-39 Guide Torrent --the highest pass rate. According to the statistics, the pass rate among our customers who prepared the exam under the guidance of our 312-39 guide torrent has reached as high as 98% to 100% with only practicing our 312-39 exam torrent for 20 to 30 hours.

>> PDF 312-39 Cram Exam <<

Test 312-39 Simulator Online - Latest 312-39 Exam Format

With the rapid development of the world economy and frequent contacts between different countries, the talent competition is increasing day by day, and the employment pressure is also increasing day by day. If you want to get a better job and relieve your employment pressure, it is essential for you to get the 312-39 Certification. However, due to the severe employment situation, more and more people have been crazy for passing the 312-39 exam by taking examinations, the exam has also been more and more difficult to pass.

EC-COUNCIL 312-39 Exam Syllabus Topics:

Topic	Details
Topic 1	• Able to develop threat cases (correlation rules), create reports • Gain a basic understanding and in-depth knowledge of security threats, attacks, vulnerabilities
Topic 2	• Gain hands-on experience in the alert triaging process • Able to prepare briefings and reports of analysis methodology and results
Topic 3	• Learn use cases that are widely used across the SIEM deployment • Gain knowledge of Incident Response Process
Topic 4	• Gain hands-on experience in SIEM use case development process • Plan, organize, and perform threat monitoring and analysis in the enterprise

Topic 5	• Gain experience and extensive knowledge of Security Information and Event Management • Able to monitor emerging threat patterns and perform security threat analysis

As the world becomes increasingly digitized, the need for cybersecurity professionals has never been greater. The EC-COUNCIL 312-39 (Certified SOC Analyst (CSA)) certification exam is the perfect way for security professionals to validate their skills and knowledge in this field. By earning this coveted certification, individuals demonstrate their ability to manage and maintain security operations centers, detect and respond to cyber threats, use various security tools, and perform vulnerability analysis.

The CSA certification is an intermediate-level certification that is ideal for professionals who are looking to advance their career in the cybersecurity field. It is particularly relevant for those who work in SOC environments, such as security analysts, incident responders, and SOC managers.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q177-Q182):

NEW QUESTION # 177
Which of the following Windows Event Id will help you monitors file sharing across the network?

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

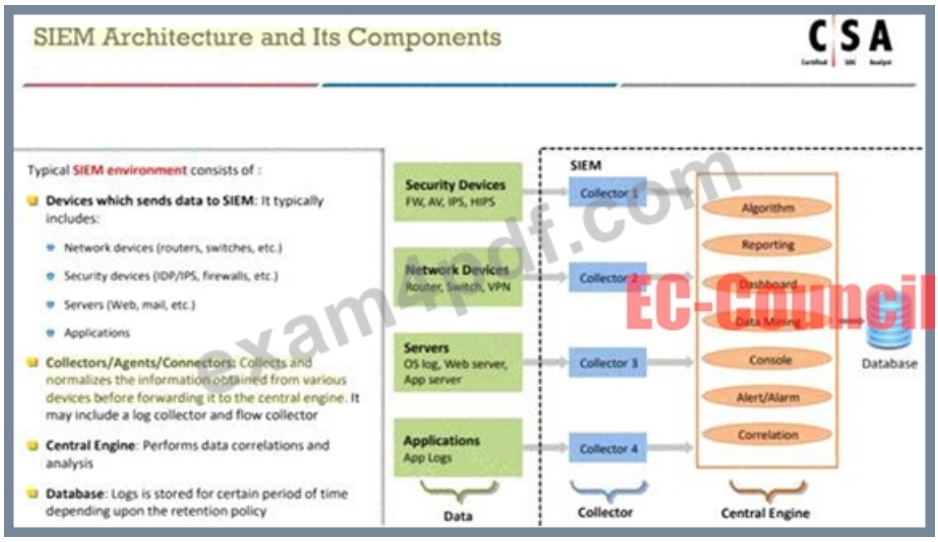
Answer: A

NEW QUESTION # 178
Which of the following are the responsibilities of SIEM Agents?
1.Collecting data received from various devices sending data to SIEM before forwarding it to the central engine.
2.Normalizing data received from various devices sending data to SIEM before forwarding it to the central engine.
3.Co-relating data received from various devices sending data to SIEM before forwarding it to the central engine.
4.Visualizing data received from various devices sending data to SIEM before forwarding it to the central engine.

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

Answer: B

Explanation:
SIEM Agents are primarily responsible for the initial stages of data processing within a SIEM system. Their duties include:
* Collecting data: SIEM Agents collect logs and other data from various devices across the network. This is a crucial step as it ensures that all relevant data is gathered for analysis.
* Normalizing data: Once the data is collected, SIEM Agents normalize it, which means they convert different log and data formats into a standardized format. This process is essential for the SIEM's central engine to analyze and correlate the data effectively.
The responsibilities of SIEM Agents generally do not include correlating data (which is typically done by the central SIEM engine) or visualizing data (which is usually a function of the SIEM's user interface or reporting tools).
References: The roles and responsibilities of SIEM Agents are outlined in EC-Council's SOC Analyst course materials and official certification guides. These resources emphasize the importance of data collection and normalization as foundational tasks performed by SIEM Agents in a Security Operations Center (SOC)12.



NEW QUESTION # 179
A SIEM alert is triggered due to unusual network traffic involving NetBIOS. The system log shows: "The TCP/IP NetBIOS Helper service entered the running state." Concurrently, Windows Security Event ID 4624 ("An account was successfully logged on") appears for multiple machines within a short time frame. The logon type is 3 (Network logon). Which of the following security incidents is the SIEM detecting?

- A. A malware infection spreading via SMB protocol
- B. A network administrator conducting routine maintenance
- C. A user connecting to shared files from multiple workstations
- D. An attacker performing lateral movement within the network

Answer: D

Explanation:
The pattern described most strongly indicates lateral movement: multiple network logons (Event ID 4624, Logon Type 3) across multiple machines in a short period, combined with NetBIOS/SMB-related service activity, suggests a host-to-host authentication pattern consistent with an attacker moving through the environment. In SOC terms, Logon Type 3 reflects network-based authentication (commonly SMB, remote service access, admin shares, or remote management). When the same source account or host triggers many network logons quickly across endpoints-especially outside normal administrative patterns-it often indicates credential abuse (pass-the-hash, stolen credentials, or remote execution frameworks). While SMB- worm propagation is possible, the scenario emphasizes authentication events across multiple machines rather than explicit malware indicators or file-write propagation patterns. Routine maintenance is plausible only with strong supporting context (approved admin accounts, change windows, known tooling), which is not provided. A single user connecting to shared files typically wouldn't generate a burst of network logons "for multiple machines" in the same way, nor would it usually coincide with suspicious NetBIOS helper state changes as an anomaly. Therefore, the best classification is attacker lateral movement within the network.

NEW QUESTION # 180
Juliea a SOC analyst, while monitoring logs, noticed large TXT, NULL payloads.
What does thisindicate?

- A. DHCP Starvation Attempt
- B. Covering Tracks Attempt
- C. DNS Exfiltration Attempt
- D. Concurrent VPN Connections Attempt

Answer: C

Explanation:
Juliea, the SOC analyst, noticed large TXT and NULL payloads in the logs. This is indicative of a DNS exfiltration attempt. DNS exfiltration is a type of cyber attack where an attacker uses the DNS protocol to sneak data out of a network undetected. It typically involves the use of large TXT records, which can be used to carry data out of the network. NULL payloads can be used in this

context to pad the DNS queries and make them less suspicious or to bypass security controls that inspect the content of DNSqueries.
The steps involved in DNS exfiltration include:
* The attacker compromises a system within the target network.
* Malware on the compromised system encodes the data it wants to exfiltrate.
* The encoded data is split into chunks that fit into DNS query sizes.
* These chunks are sent as data in DNS queries or responses, often using TXT records.
* An external attacker-controlled server receives the DNS queries and decodes the data.
References:
EC-Council's Certified SOC Analyst (CSA) course material and study guides provide detailed information on various types of cyber attacks, including DNS exfiltration.
Online resources and practice questions for the Certified SOC Analyst (CSA) exam also cover this topic and can be used to verify the answer123.
Additional information on DNS exfiltration techniques and detection methods can be found in security blogs and articles that discuss the subject in depth456.
Reference: https://www.google.com/url?
sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj8gZaKq_PuAhWGil wKHfQTC0oQFjAAegQIAR
&url=https%3A%2F%2Fconf.splunk.com%2Fsession%2F2014%
2Fconf2014_FredWilmotSanfordOwings_Splunk_Security.pdf&usg=AOvVaw3ZLfzGqM-VUG7xKtze67ac

NEW QUESTION # 181
Which of the following stage executed after identifying the required event sources?

- A. Defining Rule for the Use Case
- B. Validating the event source against monitoring requirement
- C. Implementing and Testing the Use Case
- D. Identifying the monitoring Requirements

Answer: B

NEW QUESTION # 182
.....

- Valid 312-39 Test Duration □ Answers 312-39 Real Questions □ Reliable 312-39 Exam Review □ Search for 「 312-39 」 on ✔ www.pdfvce.com □✔□ immediately to obtain a free download □312-39 Latest Test Materials
- 312-39 Pass4sure Pass Guide □ 312-39 Torrent □ 312-39 Valid Mock Exam □ Search for ⇛ 312-39 ⇚ and easily obtain a free download on □ www.exam4labs.com □ □Examcollection 312-39 Dumps Torrent
- abelbmnz522649.kylieblog.com, arunexmu574246.blogdun.com, tiffanywvsn509156.wikiexcerpt.com, kianapaol431023.blogsvirals.com, mixbookmark.com, dailybookmarkhit.com, theresatxjb468256.blogdun.com, 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, bbs.t-firefly.com, hamzailwq728684.wikiusnews.com, Disposable vapes

P.S. Free 2026 EC-COUNCIL 312-39 dumps are available on Google Drive shared by Exam4PDF: https://drive.google.com/open?id=16JocCzWOdsBaJUKqGVlabQvuCWjMmN8r