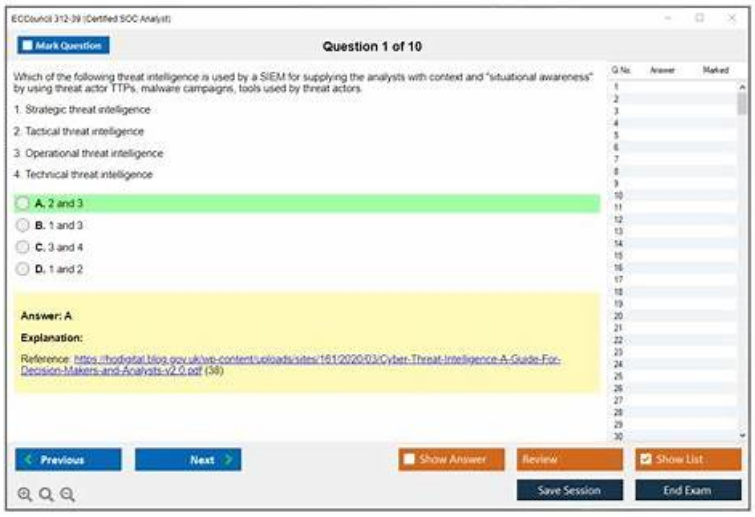
EC-COUNCIL 312-39 Exam Prep Solutions



BTW, DOWNLOAD part of ExamcollectionPass 312-39 dumps from Cloud Storage: https://drive.google.com/open?id=1rAId9-qfkCF0ItThNDxA4XMeJ09Y6d87

There is no exaggeration that you can be confident about your coming exam just after studying with our 312-39 preparation materials for 20 to 30 hours. Tens of thousands of our customers have benefited from our exam materials and passed their 312-39 exams with ease. The data showed that our high pass rate is unbelievably 98% to 100%. Without doubt, your success is 100% guaranteed with our 312-39 training guide. You will be quite surprised by the convenience to have an overview just by clicking into the link, and you can experience all kinds of 312-39 versions.

EC-COUNCIL 312-39 Certification Exam is an important certification for IT professionals who are responsible for monitoring and defending against cyber threats in a SOC environment. It is a globally recognized certification that demonstrates an individual's knowledge and skills in the field of cybersecurity and is highly valued by employers in a variety of industries.

>> Free 312-39 Dumps <<

100% Pass 2026 EC-COUNCIL Fantastic 312-39: Free Certified SOC Analyst (CSA) Dumps

Obtaining the 312-39 certificate will make your colleagues and supervisors stand out for you, because it represents your professional skills. At the same time, it will also give you more opportunities for promotion and job-hopping. The 312-39 latest exam dumps have different classifications for different qualification examinations, which can enable students to choose their own learning mode for themselves according to the actual needs of users. On buses or subways, you can use fractional time to test your learning outcomes with 312-39 Test Torrent, which will greatly increase your pro forma efficiency.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q65-Q70):

NEW QUESTION # 65
A financial services company hosts an online banking platform accessible via a public web portal. The SOC team has deployed Snort IDS to monitor HTTP traffic for potential attacks targeting the login page. One day, a user attempts to log in multiple times, generating a series of failed authentication events. During this time, Snort IDS triggers an alert based on the following rule:
alert tcp any any -> any 80 (msg:"SQL Injection attempt detected"; content:" OR T=T"; nocase; sid:1000001; rev:1;) The alert indicates that an incoming HTTP request contained the classic SQL injection payload ' OR T=T, which is commonly used to bypass login authentication by always evaluating to true. The SIEM, integrated with Snort, receives this alert and correlates it with multiple failed login attempts from the same source IP.
This triggers an automated response, temporarily blocking the suspicious IP address and notifying the SOC team. Which detection method is used by this rule?

- A. Behavioral-based detection
- B. Anomaly-based detection

- C. Statistical-based detection
- D. Signature-based detection

Answer: D

Explanation:
This rule is signature-based because it matches a known malicious pattern (a specific string payload) within network traffic. Snort's content keyword searches for an exact sequence of bytes/characters in the packet payload-in this case, a classic SQL injection tautology pattern intended to manipulate application logic.
Signature detection is high-confidence when the signature is precise and the payload is strongly associated with malicious intent. In SOC operations, signature-based rules are commonly used for well-known exploit strings, malware beacons, and protocol abuse patterns. The tradeoff is that signatures can be bypassed with encoding, obfuscation, payload variations, or different injection strategies that avoid the exact string.
Behavioral/anomaly/statistical methods, by contrast, focus on deviations from baseline or broader behavioral patterns (for example, unusual login rates, uncommon HTTP methods, or atypical data transfer volumes).
Here, the detection trigger is explicitly the presence of a known SQL injection payload string, which is the defining characteristic of signature-based detection. The SIEM correlation with failed logins adds context and confidence, but the rule itself is still signature-driven.

NEW QUESTION # 66
Which of the following technique protects from flooding attacks originated from the valid prefixes (IP addresses) so that they can be traced to its true source?

- A. Rate Limiting
- B. Throttling
- C. Egress Filtering
- D. Ingress Filtering

Answer: D

Explanation:
Ingress filtering is a technique used to ensure that incoming packets are actually from the networks that they claim to originate from. This is particularly useful in mitigating IP spoofing, where an attacker might use a legitimate IP address to send malicious packets, making it appear as though the packets are coming from a trusted source. By implementing ingress filtering, networks can check that the source IP address of incoming packets is within a range that logically should be entering the network from that point. This helps in tracing back flooding attacks to their true source and is a recommended practice to protect against such attacks.
References: The concept of ingress filtering is covered in EC-Council's Certified SOC Analyst (CSA) training and is a recognized technique for protecting against flooding attacks. It is also mentioned in the context of security operations center (SOC) processes and is a part of the knowledge base required for SOC analysts12.

NEW QUESTION # 67
Peter, a SOC analyst with Spade Systems, is monitoring and analyzing the router logs of the company and wanted to check the logs that are generated by access control list numbered 210.
What filter should Peter add to the 'show logging' command to get the required output?

- A. show logging | include 210
- B. show logging | access 210
- C. show logging | forward 210
- D. show logging | route 210

Answer: A

NEW QUESTION # 68
NationalHealth, a government agency responsible for managing sensitive patient health records, is subject to strict data sovereignty regulations requiring all data to be stored and processed within the country's borders.
Leadership is concerned about outsourcing security operations and needs complete control over patient data handling. The agency faces increasing cyber threats and requires 24/7 security monitoring. They have a large budget and can hire many security

professionals. Which SOC model is most suitable?

- A. A combination of multiple MSSPs
- B. Outsourced SOC model
- C. Hybrid SOC model (expertise of an MSSP)
- D. In-house/internal SOC model

Answer: D

Explanation:
An in-house/internal SOC model best fits when data sovereignty, strict control of sensitive data, and operational independence are the top priorities-and when the organization has the budget and staffing capacity to operate 24/7. For a government agency handling health records, limiting third-party access reduces legal, compliance, and privacy risk. An internal SOC can ensure that telemetry, incident artifacts, and investigative outputs remain within national borders and under direct governance, supporting sovereignty mandates and chain-of-custody requirements. Outsourced or multi-MSSP models increase external data exposure and often require sharing logs, incident details, or access into systems-conflicting with the requirement for complete control. A hybrid model can be effective when internal capability is limited and external expertise is needed, but the prompt explicitly states the agency can hire many professionals and wants full control. From a SOC operations perspective, an in-house SOC also allows customization of playbooks, escalation paths, and compliance reporting aligned to government standards, and it reduces dependency on vendor timelines during high-severity incidents. Therefore, the most suitable model is in-house
/internal SOC.

NEW QUESTION # 69
Identify the HTTP status codes that represents the server error.

- A. 2XX
- B. 1XX
- C. 5XX
- D. 4XX

Answer: C

NEW QUESTION # 70
.....

ExamcollectionPass has created reliable and up-to-date 312-39 Questions that help to pass the exam on the first attempt. The product is easy to use and very simple to understand ensuring it is student-oriented. The Certified SOC Analyst (CSA) dumps consist of three easy formats; The 3 formats are Desktop-based practice test software, Web-based practice exam, and PDF.

- 312-39 Exam Voucher □ 312-39 Reliable Braindumps Pdf □ 312-39 Exam Voucher □ Open [www.pdfvce.com] enter □ 312-39 □ and obtain a free download □Reliable 312-39 Exam Pattern
- 2026 Free 312-39 Dumps | Pass-Sure 100% Free New Certified SOC Analyst (CSA) Test Discount □ Search for ➤ 312-39 □ and download exam materials for free through □ www.practicevce.com □ □312-39 Test Free
- jasonomph216826.wikievia.com, tayasazb392264.blogdomago.com, friendlybookmark.com, setbookmarks.com, theozabm787171.blog-eye.com, susantuyw418204.dekaronwiki.com, orangebookmarks.com, bbs.ucwm.com, andrewtcrx986654.blogproducer.com, phoenixashg726265.wikiap.com, Disposable vapes

2026 Latest ExamcollectionPass 312-39 PDF Dumps and 312-39 Exam Engine Free Share: https://drive.google.com/open?id=1rAId9-qfkCF0ItThNDxA4XMeJ09Y6d87