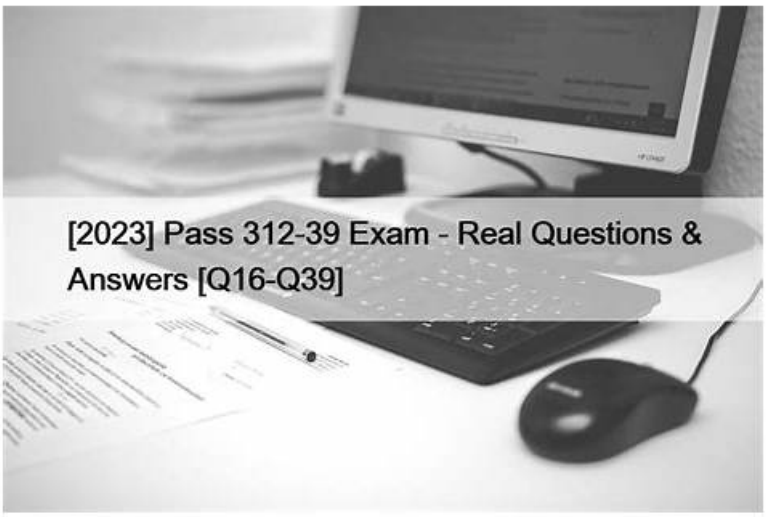
Exam 312-39 Questions Answers - New 312-39 Exam Online



2026 Latest BraindumpQuiz 312-39 PDF Dumps and 312-39 Exam Engine Free Share: https://drive.google.com/open?id=1G-3Ll49I5TkxhehtSaok-3XxkVDZ9_Ss

In order to help our candidates know better on our 312-39 exam questions to pass the exam, we provide you the responsible 24/7 service. Our candidates might meet different problems on 312-39 learing guide during purchasing and using our 312-39 prep guide, you can contact with us through the email, and we will give you respond and solution as quick as possible. With the commitment of helping candidates to Pass 312-39 Exam, we have won wide approvals by our clients. We always take our candidates' benefits as the priority, so you can trust us without any hesitation.

What's Leading Certification Path?

As detailed above, passing the EC-Council 312-39 Exam will qualify you for the aforementioned Certified SOC Analyst (CSA) certificate. This is a detailed certification path that emphasizes the skills and concepts needed to build a lasting career through continuous knowledge enhancement and training using the best study materials. This track suits all IT specialists who are keen to contribute to a SOC team and know their stuff in this field. With the rapid expansion of the security landscape, building exceptional SOC teams is becoming every organization's biggest priority as the focus shifts to actively responding to security incidents instead of simply recognizing them. Thus, getting this certificate will easily turn you into a first-line "soldier" tasked with warning the team members of potential security attacks and mitigating the same if necessary.

>> Exam 312-39 Questions Answers <<

EC-COUNCIL 312-39 Practice Test - Free Updated Demo (2026)

BraindumpQuiz makes your investment 100% secure when you purchase 312-39 practice exams. We guarantee your success in the 312-39 exam. Otherwise, our full refund policy will enable you to get your money back. The practice exams for EC-COUNCIL CSA are prepared by the 312-39 subject experts who are well aware of the 312-39 exam syllabus requirements. Our Customer support team is 24/7 available that you can reach through email or Live Chat for any 312-39 exam preparation product related question.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q151-Q156):

NEW QUESTION # 151
Which of the following process refers to the discarding of the packets at the routing level without informing the source that the data did not reach its intended recipient?

- A. Load Balancing
- B. Drop Requests

- C. Rate Limiting
- D. Black Hole Filtering

Answer: D

Explanation:
Black hole filtering is a network security measure used to prevent unwanted or malicious traffic from entering a network. It works by directing traffic to a null interface, a non-existent server, or a black hole IP address where the packets are dropped without acknowledgment. This process is typically used to protect against denial-of-service (DoS) attacks, where an overwhelming amount of traffic is sent to a network with the intent to disrupt service.
In the context of a security operations center (SOC), black hole filtering can be an effective strategy for mitigating threats. When a threat is identified, such as a DoS attack, the SOC analyst can configure the network to redirect the suspicious traffic to a black hole, effectively neutralizing the attack by preventing the malicious data packets from reaching their intended target.
References: The EC-Council's Certified SOC Analyst (C|SA) program covers various defensive strategies, including black hole filtering, as part of its curriculum for Tier I and Tier II SOC analysts. The program emphasizes the importance of understanding and implementing network security measures to protect against cyber threats12.
Reference:https://en.wikipedia.org/wiki/Black_hole_(networking)#:~:text=In%20networking%2C%20black%20holes%20refer,not%20reach%20its%20intended%20recipient.

NEW QUESTION # 152
Mike is an incident handler for PNP Infosystems Inc. One day, there was a ticket raised regarding a critical incident and Mike was assigned to handle the incident. During the process of incident handling, at one stage, he has performed incident analysis and validation to check whether the incident is a true incident or a false positive.
Identify the stage in which he is currently in.

- A. Incident Recording and Assignment
- B. Incident Disclosure
- C. Incident Triage
- D. Post-Incident Activities

Answer: A

NEW QUESTION # 153
A manufacturing company is deploying a SIEM system and uses an output-driven approach, starting with use cases addressing unauthorized access to production control systems. They configure data sources and alerts to ensure actionable alerts with low false positives, then expand to supply chain disruptions and malware detection. What is the primary advantage of an output-driven approach?

- A. The company can collect logs from non-critical systems.
- B. The SIEM system can automatically block all unauthorized access attempts.
- C. The company can create more complex use cases with greater scope.
- D. The SOC team can respond to all incidents in real time without delays.

Answer: C

Explanation:
An output-driven SIEM deployment builds capability by starting with a narrowly defined, high-value detection outcome and then expanding once success is proven. The primary advantage is that it supports iterative growth into broader and more complex use cases with confidence. Each validated use case forces disciplined work on prerequisites: correct data onboarding, parsing, field normalization, baseline understanding, and tuning to reduce false positives. That foundation enables more advanced scenarios that require richer correlation (for example, linking identity events, network telemetry, endpoint behavior, and application logs) and often cover longer timelines or more complex workflows, such as supply chain disruption detection. Option A is not an advantage; collecting logs from non-critical systems may or may not be required depending on use cases. Option C is unrealistic because response speed depends on staffing and workflows, not only SIEM deployment strategy. Option D implies active prevention, which is not the SIEM's core role (it can trigger automation, but blocking is not automatic by default). Therefore, the best advantage among the given options is enabling creation and expansion to more complex use cases with wider scope.

NEW QUESTION # 154
Where will you find the reputation IP database, if you want to monitor traffic from known bad IP reputation using OSSIM SIEM?

- A. /etc/ossim/reputation
- B. /etc/siem/ossim/server/reputation.data
- C. /etc/ossim/server/reputation.data
- D. /etc/ossim/siem/server/reputation/data

Answer: C

Explanation:
In OSSIM SIEM, the reputation IP database is a crucial component for monitoring traffic from known malicious IP addresses. The correct location of this database is:
* /etc/ossim/server/reputation.data: This directory and file name specify the location where the reputation database is stored. It contains the list of known bad IP addresses that the OSSIM system uses to monitor and identify potentially harmful traffic.
* Purpose of the Reputation Database: The database is used to compare incoming traffic against the list of known bad IPs. If a match is found, OSSIM can generate alerts or take predefined actions to mitigate the threat.
* Updating the Database: It's important to regularly update the reputation database to ensure it includes the latest threat intelligence. This helps maintain the effectiveness of the SIEM system in identifying and responding to threats.
References: The information provided here is based on standard OSSIM documentation and best practices for SIEM systems as outlined in EC-Council's SOC Analyst study materials1234.
Please note that while I strive to provide accurate information, it's always best to consult the latest EC- Council SOC Analyst documents and learning resources for the most current and detailed guidance.
Graphical user interface, text Description automatically generated

NEW QUESTION # 155
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

Explanation:
The WindowsEvent ID 5140 is used to monitor file sharing across a network. This event is triggered every time a network share object is accessed, and it generates once per session when the first access attempt is made. It is part of the Audit File Share category and provides information about the access, including the user and device that accessed the share, the network address from which the access was made, and the name of the share that was accessed.
References:The information about Event ID 5140 can be found in the Microsoft documentation for Windows security auditing, specifically under the Advanced security audit policies related to Audit File Share1.
Reference: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=5140

NEW QUESTION # 156
.....

- 312-39 Technical Training □ Valid Test 312-39 Test □ New 312-39 Test Sims □ Immediately open " www.pdfvce.com " and search for ➡ 312-39 □□□ to obtain a free download □312-39 Reliable Test Duration
- Prepares you for the format of your 312-39 exam dumps □ Open " www.examdiscuss.com " and search for ✔ 312-39 □✔□ to download exam materials for free □Valid Braindumps 312-39 Ebook
- Certified SOC Analyst (CSA) sure torrent - 312-39 valid training - Certified SOC Analyst (CSA) test pdf □ Search on 【 www.pdfvce.com 】 for 《 312-39 》 to obtain exam materials for free download □312-39 Reliable Test Duration
- 312-39 Dumps Discount □ 312-39 Reliable Study Notes □ 312-39 Technical Training □ Immediately open " www.prep4sures.top " and search for □ 312-39 □ to obtain a free download □312-39 Technical Training
- Pass Guaranteed Quiz Professional EC-COUNCIL - Exam 312-39 Questions Answers □ Open ▷ www.pdfvce.com ◁ and search for （ 312-39 ） to download exam materials for free □Latest 312-39 Training
- Exam 312-39 Dumps □ Valid Braindumps 312-39 Ebook □ Valid Test 312-39 Test □ Search for ➥ 312-39 □ and download it for free immediately on □ www.dumpsquestion.com □ □312-39 Exam Overviews
- Pass Guaranteed 2026 High Pass-Rate EC-COUNCIL Exam 312-39 Questions Answers □ Copy URL ➤ www.pdfvce.com □ open and search for ▸ 312-39 ◂ to download for free □312-39 Exam Score
- Latest 312-39 Training □ 312-39 Updated Dumps ↙ 312-39 Reliable Test Duration □ Search on 「 www.exam4labs.com 」 for □ 312-39 □ to obtain exam materials for free download □Exam 312-39 Dumps
- extrabookmarking.com, nimmansocial.com, nellpfog324843.dgbloggers.com, haimadjln451401.dailyblogzz.com, philippvpu708998.bloggactivo.com, thesocialdelight.com, larissaeftv840211.wizzardsblog.com, haleemakqhj990956.qodsblog.com, phoenixzomp144466.wikikarts.com, bookmarkingdelta.com, Disposable vapes

BONUS!!! Download part of BraindumpQuiz 312-39 dumps for free: https://drive.google.com/open?id=1G-3Ll49I5TkxhehtSaok-3XxkVDZ9_Ss