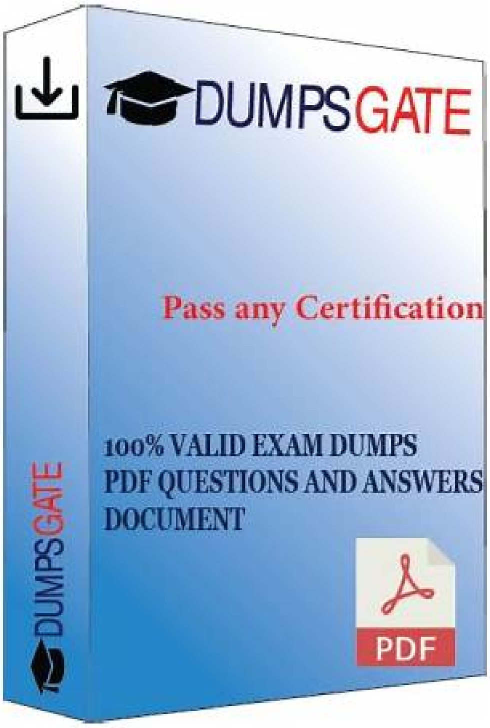
# Latest 312-39 Exam Dumps & 312-39 Reliable Exam Syllabus



DOWNLOAD the newest It-Tests 312-39 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1s_z2IMnbEsIdV9eJR8rW1K5HXo2R2PSO

Free update for 365 days is available if you buy 312-39 exam braindumps from us. That is to say, in the following year, you can get the latest information about the 312-39 exam dumps timely. And the update version will be sent to your email automatically. In addition, the 312-39 Exam Braindumps are compiled by experienced experts who are quite familiar with the dynamics about the exam center, therefore the quality and accuracy of the 312-39 exam braindumps can be guaranteed.

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.

**>> Latest 312-39 Exam Dumps <<**

## Hot Latest 312-39 Exam Dumps Pass Certify | Efficient 312-39 Reliable Exam Syllabus: Certified SOC Analyst (CSA)

It-Tests also offers a demo of the EC-COUNCIL 312-39 exam product which is absolutely free. Up to 1 year of free Certified SOC Analyst (CSA) (312-39) questions updates are also available if in any case the sections of the EC-COUNCIL 312-39 actual test changes after your purchase. Lastly, we also offer a full refund guarantee according to terms and conditions if you do not get success in the Certified SOC Analyst (CSA) Certification Exam after using our 312-39 product. These offers by It-Tests save your time and money. Buy Certified SOC Analyst (CSA) (312-39) practice material today.

## EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q69-Q74):

**NEW QUESTION # 69**
InfoSystem LLC, a US-based company, is establishing an in-house SOC. John has been given the responsibility to finalize strategy, policies, and procedures for the SOC.
Identify the job role of John.

- A. Security Analyst - L1
- B. Security Engineer
- C. Security Analyst - L2
- D. Chief Information Security Officer (CISO)

**Answer: D**

Explanation:
The role offinalizing strategy, policies, and procedures for a Security Operations Center (SOC) typically falls under the responsibilities of a Chief Information Security Officer (CISO). The CISO is a senior-level executive within an organization who coordinates and manages the overall strategy and defense mechanisms to protect the organization's information and technology assets. This role involves leadership and strategic decision-making, which includes establishing the SOC's framework, defining its policies, and overseeing its procedures.
References: The EC-Council provides various resources and guides that outline the roles and responsibilities within a SOC. According to the information available, a Security Analyst, whether Level 1 or Level 2, isprimarily responsible for monitoring and analyzing the organization's security posture on a continuous basis. A Security Engineer focuses on the design and implementation of security systems. In contrast, the CISO role encompasses a broader scope of strategic leadership and management, which aligns with the responsibilities described for John in the scenario12.
Reference: https://www.exabeam.com/security-operations-center/security-operations-center-roles-and- responsibilities/

**NEW QUESTION # 70**
Juliea a SOC analyst, while monitoring logs, noticed large TXT, NULL payloads.
What does this indicate?

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

**Answer: D**

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 DNS queries.
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.

**NEW QUESTION # 71**
John, a threat analyst at GreenTech Solutions, wants to gather information about specific threats against the organization. He started collecting information from various sources, such as humans, social media, chat room, and so on, and created a report that contains malicious activity.
Which of the following types of threat intelligence did he use?

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

**Answer: D**

Explanation:
Operational threat intelligence involves gathering detailed information about specific threats to an organization. It is often derived from various sources, including human intelligence, social media, chat rooms, and other platforms where data about malicious activities can be collected. This type of intelligence is focused on understanding the specifics of a threat, such as the tactics, techniques, and procedures (TTPs) of threat actors, and is used to inform the organization about imminent or ongoing attacks.
In the scenario described, John, a threat analyst, is collecting information from diverse sources to create a report on malicious activity. This aligns with the practices of operational threat intelligence, which is concerned with the details of particular threats and activities, rather than broader strategic trends or technical indicators.
References:The EC-Council's Certified Threat Intelligence Analyst (C|TIA) program provides comprehensive training on the different types of threat intelligence, including operational threat intelligence. The program covers the methodologies for collecting, analyzing, and disseminating threat intelligence, which are relevant to the activities performed by John in the scenario1.

**NEW QUESTION # 72**
According to the Risk Matrix table, what will be the risk level when the probability of an attack is very low and the impact of that attack is major?

- A. Medium
- B. Extreme
- C. High
- D. Low

**Answer: D**

**NEW QUESTION # 73**
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. Rate Limiting
- B. Black Hole Filtering
- C. Drop Requests
- D. Load Balancing

**Answer: B**

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.

**NEW QUESTION # 74**

......

Our 312-39 study materials are compiled by domestic first-rate experts and senior lecturer and the contents of them contain all the important information about the test and all the possible answers of the questions which maybe appear in the test. You can use the practice test software to check your learning outcomes. Our 312-39 study materials' self-learning and self-evaluation functions, the statistics report function, the timing function and the function of stimulating the test could assist you to find your weak links, check your level, adjust the speed and have a warming up for the real exam. You will feel your choice to buy 312-39 Study Materials are too right.

**312-39 Reliable Exam Syllabus**: https://www.it-tests.com/312-39.html

- 312-39 Dumps Download □ 312-39 Guaranteed Questions Answers □ 312-39 Guaranteed Questions Answers □ The page for free download of □ 312-39 □ on ➡ www.troytecdumps.com □□□ will open immediately □312-39 Valid Dumps Ppt
- EC-COUNCIL 312-39 Dumps PDF Format Is Best For Instant Preparation □ Download ➡ 312-39 □□□ for free by simply entering ▹ www.pdfvce.com ◃ website □312-39 Valid Study Notes
- Latest 312-39 Test Pass4sure □ Latest 312-39 Test Pass4sure □ Interactive 312-39 Course □ Open ➥ www.prep4away.com □ and search for ☀ 312-39 □☀□ to download exam materials for free □312-39 Test Question
- Hot Latest 312-39 Exam Dumps | Professional 312-39 Reliable Exam Syllabus: Certified SOC Analyst (CSA) 100% Pass □ □ Go to website ✔ www.pdfvce.com □✔□ open and search for ➠ 312-39 □ to download for free □Valid 312-39 Study Materials
- Guide 312-39 Torrent □ Valid 312-39 Study Materials □ 312-39 Latest Test Question □ Download ▸ 312-39 ◂ for free by simply searching on ▸ www.troytecdumps.com ◂ □312-39 Dumps Download
- Guide 312-39 Torrent □ 312-39 Test Question □ Valid 312-39 Torrent □ Search on " www.pdfvce.com " for 《 312-39 》 to obtain exam materials for free download □312-39 Valid Exam Fee
- Valid 312-39 Torrent □ Interactive 312-39 Course □ Valid 312-39 Torrent □ Search for （ 312-39 ） on ☀ www.dumpsmaterials.com □☀□ immediately to obtain a free download □Intereactive 312-39 Testing Engine
- 312-39 Valid Exam Fee □ 312-39 Practice Tests □ Practice 312-39 Questions □ Search on " www.pdfvce.com " for 「 312-39 」 to obtain exam materials for free download □Valid 312-39 Torrent
- Hot Latest 312-39 Exam Dumps | Professional 312-39 Reliable Exam Syllabus: Certified SOC Analyst (CSA) 100% Pass □ Download " 312-39 " for free by simply searching on ⇛ www.vce4dumps.com ⇚ □312-39 Test Question
- 312-39 Dumps Download □ Intereactive 312-39 Testing Engine □ Guide 312-39 Torrent □ Immediately open ➽ www.pdfvce.com □ and search for ➤ 312-39 □ to obtain a free download □Interactive 312-39 Course
- 312-39 Guaranteed Questions Answers □ 312-39 Questions Pdf □ 312-39 Trustworthy Source □ Search for ➤ 312-39 □ and download exam materials for free through " www.exam4labs.com " □312-39 Practice Tests
- bbs.t-firefly.com, soulroutes.org.in, 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, 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, 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, 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, Disposable vapes

BONUS!!! Download part of It-Tests 312-39 dumps for free: https://drive.google.com/open?id=1s_z2IMnbEsIdV9eJR8rW1K5HXo2R2PSO