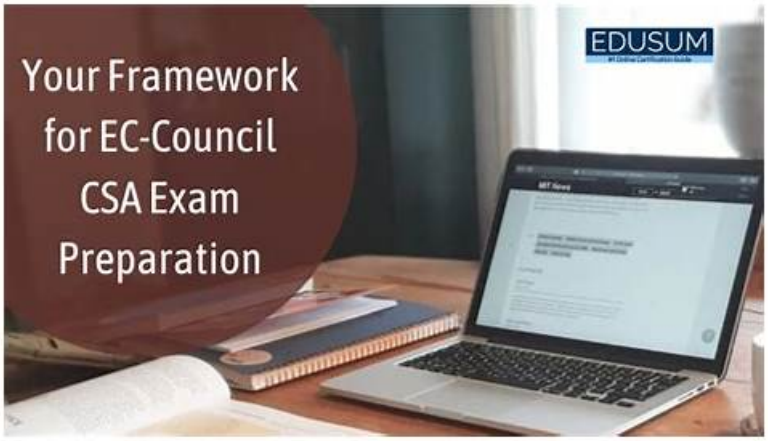
Quiz 2026 EC-COUNCIL 312-39–Trustable Exam Quick Prep



What's more, part of that RealVCE 312-39 dumps now are free: https://drive.google.com/open?id=1Myya51FfaPJ2sGu5g7iIJtHzEXgGh9VA

With these mock exams, it is easy to track your progress by monitoring your marks each time you go through the 312-39 practice test. Our 312-39 practice exams will give you an experience of attempting the 312-39 original examination. You will be able to deal with the actual exam pressure better when you have already experienced it in our EC-COUNCIL 312-39 practice exams.

Candidates who pass the CSA exam will be able to demonstrate their ability to perform tasks such as analyzing security events, identifying security incidents, and managing security incidents to resolution. They will also be able to demonstrate their knowledge of various security frameworks and regulations, such as NIST, CIS Critical Security Controls, and GDPR. Overall, this certification provides candidates with the skills and knowledge required to become a successful SOC analyst and make significant contributions to an organization's security posture.

EC-COUNCIL 312-39 Certified SOC Analyst (CSA) certification exam is a crucial step for IT and security professionals who aim to build a career in security operations centers (SOC). Certified SOC Analyst (CSA) certification is designed to validate the candidate's knowledge and skills related to SOC operations, including threat detection, response, and mitigation. 312-39 exam focuses on a wide range of topics, including security operations, incident management, threat intelligence, and risk management.

>> Exam 312-39 Quick Prep <<

312-39 Latest Exam Dumps & 312-39 Verified Study Torrent & 312-39 Practice Torrent Dumps

Rather than pretentious help for customers, our after-seals services are authentic and faithful. Many clients cannot stop praising us in this aspect and become regular customer for good. We have strict criterion to help you with the standard of our 312-39 training materials. Our company has also being Customer First. So we consider the facts of your interest firstly. All the preoccupation based on your needs and all these explain our belief to help you have satisfactory and comfortable purchasing services. We assume all the responsibilities our 312-39 simulating practice may bring you foreseeable outcomes and you will not regret for believing in us assuredly.

The EC-Council Certified SOC Analyst (CSA) certification is a comprehensive program that tests the skills and knowledge required to effectively monitor, detect, and respond to security incidents in real-time. The CSA certification covers the essential skills required to work in a Security Operations Center (SOC) and is designed for professionals who want to enhance their knowledge of security operations, incident response, and threat intelligence.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q188-Q193):

NEW QUESTION # 188
As a SOC Administrator at a mid-sized financial institution, you noticed intermittent network slowdowns and unexplained high memory usage across multiple critical systems. Your initial analysis found no traces of malware, but a forensic investigation revealed

unauthorized scheduled tasks that executed during off-peak hours. These tasks ran obfuscated scripts that connected to an external command-and-control (C2) server.
Further investigations showed that the adversary had gained access months ago through a compromised VPN account, leveraging stolen credentials from a phishing campaign. Which phase of the Advanced Persistent Threat (APT) lifecycle does this scenario align with?

- A. Search and Exfiltration
- B. Persistence
- C. Cleanup
- D. Initial Intrusion

Answer: B

Explanation:
This scenario best aligns with Persistence because the attacker established mechanisms to maintain access over time after the initial compromise. The defining evidence is "unauthorized scheduled tasks executed during off-peak hours" running obfuscated scripts and connecting to a C2 server. Scheduled tasks and startup mechanisms are classic persistence techniques that allow an adversary to survive reboots, re-establish footholds, and perform recurring actions (beaconing, payload retrieval, credential harvesting) without continuous interactive access. The scenario explicitly states the adversary gained access months ago via compromised VPN credentials (initial intrusion), but what you are observing now is the long-lived foothold and automated re-entry capability. Cleanup would involve covering tracks and removing evidence; while obfuscation and potential log manipulation can be related, the core described behavior is recurring execution and ongoing C2 communication. Search and exfiltration would focus on data discovery and transfer; while network slowdowns could be related to exfiltration, the most direct indicators here are persistence mechanisms enabling continued control. For SOC response, this phase emphasizes removing persistence artifacts, rotating credentials, and validating no alternate footholds remain.

NEW QUESTION # 189
What is the process of monitoring and capturing all data packets passing through a given network using different tools?

- A. Network Scanning
- B. Network Sniffing
- C. DNS Footprinting
- D. Port Scanning

Answer: B

Explanation:
Network sniffing is the process of monitoring and capturing all data packets passing through a given network.
This is typically done using specialized software or hardware tools designed for this purpose. Here's a detailed explanation of the process:
* Monitoring Traffic: Network sniffing involves using a tool to monitor the data flowing over the network. This can include all types of data packets, regardless of where they come from or where they are going.
* Capturing Packets: The tool captures each packet that passes through the network. This includes the packet's header, which contains information about the packet's source, destination, and other metadata, as well as the payload, which is the actual data being transmitted.
* Analysis: Once captured, the packets can be analyzed for various purposes, such as troubleshooting network issues, monitoring network performance, or detecting security threats.
* Tools Used: There are many tools available for network sniffing, with Wireshark being one of the most popular and widely used due to its powerful features and flexibility1.
References: The concept of network sniffing is covered in EC-Council's Certified SOC Analyst (CSA) training and certification program, which includes understanding the use of tools like Wireshark for packet capturing and analysis213.
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.

NEW QUESTION # 190
Sarah, a financial analyst at a multinational corporation, is suspected of leaking sensitive financial data to an unauthorized external party. The SOC team observed anomalous data transfer patterns originating from her account, flagged by the SIEM, indicating potential data exfiltration. The incident response team must contain the incident swiftly to minimize data loss and protect critical assets. As a SOC analyst, which should be prioritized as the initial containment measure?

- A. Data-Centric Audit and Protection (DCAP)
- B. Change passwords regularly
- C. Isolate the storage
- D. Access control

Answer: D

Explanation:
Initial containment for suspected data exfiltration by a specific user account should prioritize immediately restricting that account's ability to access and transfer data. "Access control" is the broad containment category that includes disabling the account, suspending sessions, revoking tokens, removing access to sensitive shares, and applying conditional access blocks. This is the fastest way to stop ongoing data loss while preserving evidence for investigation. "Change passwords regularly" is a general security hygiene practice, not an initial incident containment action, and it may not stop exfiltration quickly if active sessions or tokens remain valid. "Isolate the storage" can be appropriate if a particular repository is being actively exfiltrated, but it can be disruptive to business operations and may not address the actor's continued access paths across other systems. DCAP is a programmatic capability for monitoring and controlling data access over time; it is valuable, but it is not the immediate first step when the SOC must rapidly stop suspected exfiltration. From a SOC playbook view, the initial action is to reduce attacker/insider access immediately (account restriction), then scope what data was accessed, preserve logs, and coordinate with HR/legal for insider procedures.

NEW QUESTION # 191
Where will you find the reputation IP database, if you want to monitor traffic from known bad IP reputation using OSSIM SIEM?

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

Answer: C

NEW QUESTION # 192
Shawn is a security manager working at Lee Inc Solution. His organization wants to develop threat intelligent strategy plan. As a part of threat intelligent strategy plan, he suggested various components, such as threat intelligence requirement analysis, intelligence and collection planning, asset identification, threat reports, and intelligence buy-in.
Which one of the following components he should include in the above threat intelligent strategy plan to make it effective?

- A. Threat pivoting
- B. Threat trending
- C. Threat boosting
- D. Threat buy-in

Answer: B

Explanation:
In the context of a threat intelligence strategy plan, 'threat trending' is a critical component that should be included to make the plan effective. Threat trending involves analyzing data over time to identify patterns and trends in cyber threats. This allows an organization to anticipate potential future attacks and prepare accordingly. It is an essential part of a proactive threat intelligence program, enabling the organization to stay ahead of threats rather than just reacting to them.
The other options, while they may be relevant in certain contexts, are not as central to the development of a threat intelligence strategy plan as 'threat trending' is. 'Threat pivoting' refers to the process of using one piece of data to uncover more data (e.g., using an IP address to find related domains). 'Threat buy-in' is not a standard term in threat intelligence, but it could refer to gaining organizational support for threat intelligence efforts. 'Threat boosting' is not a recognized term in the field of cybersecurity.
References: The answer is derived from the components of a threat intelligence strategy as outlined in the EC-Council's Certified SOC Analyst (CSA) training and certification program, which emphasizes the importance of understanding and implementing a threat intelligence-driven SOC12. The CSA program also covers the use of threat intelligence for enhanced incident detection1. The EC-Council materials highlight the need for SOC analysts to understand various types of cyber threats and the importance of threat intelligence in detecting and responding to these threats2.

NEW QUESTION # 193

.....

Latest 312-39 Test Testking: https://www.realvce.com/312-39_free-dumps.html

- Reliable 312-39 Exam Sims □ 312-39 Latest Dumps □ Real 312-39 Exams □ Easily obtain ➠ 312-39 □ for free download through " www.practicevce.com " □Reliable 312-39 Exam Guide
- 312-39 Exam Cram □ 312-39 Valid Real Exam □ 312-39 Latest Dumps □ Search on ☀ www.pdfvce.com □☀□ for □ 312-39 □ to obtain exam materials for free download □Practice 312-39 Exam Fee
- 312-39 Reliable Test Testking □ 312-39 Valid Real Exam □ 312-39 Exam Cram □ " www.prep4sures.top " is best website to obtain ✔ 312-39 □✔□ for free download □Valid 312-39 Test Camp
- First-grade Exam 312-39 Quick Prep to Obtain EC-COUNCIL Certification □ Immediately open ➡ www.pdfvce.com □□□ and search for ➠ 312-39 □ to obtain a free download □312-39 Free Vce Dumps
- Valid 312-39 Test Camp □ Reliable 312-39 Exam Guide ❤ Reliable 312-39 Test Labs □ Easily obtain ✔ 312-39 □✔□ for free download through ✔ www.troytecdumps.com □✔□ □Reliable 312-39 Exam Guide
- 312-39 Valid Real Exam □ 312-39 Reliable Test Testking □ Reliable 312-39 Test Labs □ Enter ➤ www.pdfvce.com □ and search for ⇛ 312-39 ⇚ to download for free □Reliable 312-39 Test Pattern
- Flexible 312-39 Testing Engine !! Reliable 312-39 Exam Guide □ Flexible 312-39 Testing Engine □ Download □ 312-39 □ for free by simply entering ➽ www.examcollectionpass.com □ website □312-39 Reliable Test Testking
- Latest 312-39 Exam Discount □ 312-39 Free Vce Dumps □ Valid 312-39 Test Camp □ Go to website □ www.pdfvce.com □ open and search for ➠ 312-39 □ to download for free □Valid 312-39 Test Notes
- Reliable 312-39 Exam Guide □ Latest 312-39 Exam Discount □ Reliable 312-39 Exam Sims □ Easily obtain free download of （ 312-39 ） by searching on □ www.examcollectionpass.com □ □Reliable 312-39 Test Pattern
- Free PDF 2026 EC-COUNCIL 312-39: Certified SOC Analyst (CSA) Newest Exam Quick Prep □ Search for □ 312-39 □ and download it for free on 【 www.pdfvce.com 】 website □312-39 Valid Real Exam
- 312-39 Exam Cram □ Flexible 312-39 Testing Engine □ 100% 312-39 Exam Coverage □ Open ⇛ www.pass4test.com ⇚ enter □ 312-39 □ and obtain a free download ♥312-39 Latest Dumps
- alexiarzzh010994.wizzardsblog.com, anitadtik084363.smblogsites.com, bookmarkingace.com, kianahqbq082195.blogofchange.com, bookmarkstime.com, katrinahwwn604991.blogspothub.com, substack.com, nicolexmws519239.blogthisbiz.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, ellauxqx619265.fliplife-wiki.com, Disposable vapes

BTW, DOWNLOAD part of RealVCE 312-39 dumps from Cloud Storage: https://drive.google.com/open?id=1Myya51FfaPJ2sGu5g7iIJtHzEXgGh9VA