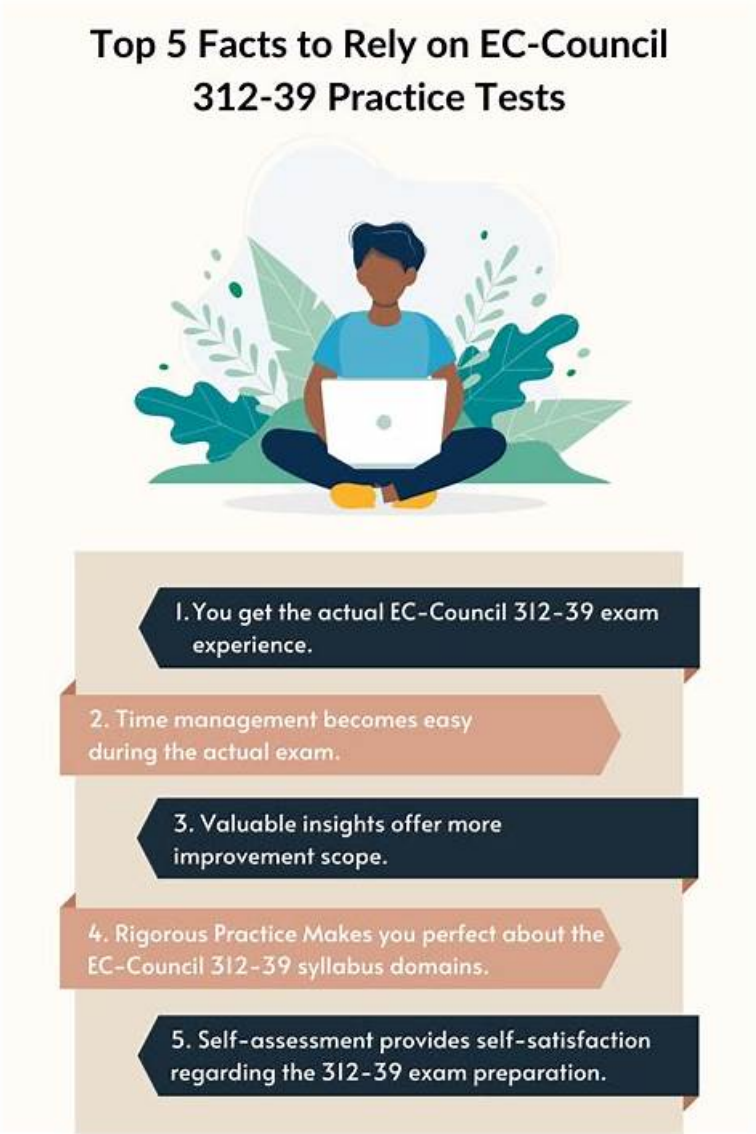
Reliable 312-39 Cram Materials, New 312-39 Exam Online



DOWNLOAD the newest PassTestking 312-39 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=10gVjF_V1oT3eWV86qfj259Njra3YMhQk

As is known to all, 312-39 practice test simulation plays an important part in the success of exams. By simulation, you can get the hang of the situation of the real exam with the help of our free demo of 312-39 exam questions. Just as an old saying goes, knowing the enemy and yourself, you can fight a hundred battles with no danger of defeat. Simulation of our 312-39 Training Materials make it possible to have a clear understanding of what your strong points and weak points are and at the same time, you can learn comprehensively about the 312-39 exam and pass it easily.

EC-COUNCIL 312-39 exam is a vendor-neutral certification, which means that it is not tied to any specific technology or product. Certified SOC Analyst (CSA) certification is recognized globally, and its holders are highly valued by employers. The CSA certification helps candidates to stand out in the competitive job market and improve their chances of getting hired or promoted in their current job.

EC-COUNCIL is a leading organization that provides cybersecurity training and certification programs worldwide. One of the most popular certifications offered by EC-COUNCIL is the Certified SOC Analyst (CSA) certification. The CSA certification exam, also known as the 312-39 Exam, is designed to test the knowledge and skills of candidates in the field of security operations center (SOC) analysis.

>> Reliable 312-39 Cram Materials <<

New 312-39 Exam Online - 312-39 Exam Pass Guide

EC-COUNCIL certification 312-39 exam is a test of IT professional knowledge. PassTestking is a website which can help you quickly pass EC-COUNCIL certification 312-39 exams. In order to pass EC-COUNCIL certification 312-39 exam, many people who attend EC-COUNCIL certification 312-39 exam have spent a lot of time and effort, or spend a lot of money to participate in the cram school. PassTestking is able to let you need to spend less time, money and effort to prepare for EC-COUNCIL Certification 312-39 Exam, which will offer you a targeted training. You only need about 20 hours training to pass the exam successfully.

The CSA certification is recognized globally and is highly valued by organizations looking to hire SOC analysts. Certified SOC Analyst (CSA) certification demonstrates that the individual has the necessary knowledge and skills to protect organizations against cyber threats. It also validates the individual's ability to respond to security incidents and mitigate the risks associated with these incidents.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q105-Q110):

NEW QUESTION # 105
Which of the following Windows event is logged every time when a user tries to access the "Registry" key?

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

Answer: D

Explanation:
The Windows event that is logged when a user tries to access a "Registry" key is identified by the event ID 4657. This event ID corresponds to the modification of a registry value. Here's how the process is tracked and logged:
* Detection: The system monitors access to registry keys and values.
* Logging: If a user accesses a registry key, and the key's audit policy is set to log such events, the event is logged.
* Event ID 4657: This specific event ID is used to denote that a registry value was modified, which includes creation, modification, and deletion of registry values.
* Audit Policy: For the event to be logged, "Set Value" auditing must be enabled in the registry key's System Access Control List (SACL).
References: The EC-Council SOC Analyst course materials and study guides detail the various Windows event IDs and their significance in monitoring and analyzing security events. Event ID 4657 is specifically covered as part of the curriculum that deals with registry access monitoring and logging1. Additionally, Microsoft's official documentation provides comprehensive information on this event ID and its role in security auditing2.

NEW QUESTION # 106
What does the Security Log Event ID 4624 of Windows 10 indicate?

- A. A share was assessed
- B. New process executed
- C. Service added to the endpoint
- D. An account was successfully logged on

Answer: D

Explanation:
The Security Log Event ID 4624 in Windows 10 indicates that an account was successfully logged on. This event is generated when a logon session is created, which could be due to a user logging on to the system, a service starting, or a scheduled task running. It is a critical event for security monitoring as it can help in identifying unauthorized access to the system.
References This information is consistent with the official Microsoft documentation and security guidelines, which can be found in the EC-Council's Certified SOC Analyst (CSA) course materials and study guides, specifically in the sections discussing the auditing and monitoring of security log events.

NEW QUESTION # 107
In which phase of Lockheed Martin's - Cyber Kill Chain Methodology, adversary creates a deliverable malicious payload using an exploit and a backdoor?

- A. Exploitation
- B. Weaponization
- C. Reconnaissance
- D. Delivery

Answer: B

Explanation:
In the Lockheed Martin Cyber Kill Chain Methodology, the phase where an adversary creates a deliverable maliciouspayload using an exploit and a backdoor is known as the Weaponization phase. This is the second stage of the Cyber Kill Chain, which occurs after the initial Reconnaissance phase. During Weaponization, the attacker prepares a malicious payload that is designed to exploit vulnerabilities in the target system. This payload often includes a backdoor to allow for persistent access to the compromised system. The Weaponization phase involves the creation of malware tailored to the target's specific vulnerabilities discovered during Reconnaissance. The attacker uses this malware to create a weaponized deliverable, which can be transmitted to the target during the subsequent Delivery phase of the Cyber Kill Chain.
References: The EC-Council SOC Analyst course materials and study guides discuss the Cyber Kill Chain Methodology in detail, including the Weaponization phase. These resources are designed to provide SOC Analysts with the knowledge and skills necessary to identify, analyze, and respond to cyber threats effectively. For further information, please refer to the official EC-Council Certified SOC Analyst (CSA) study guides and related course materials. Additionally, Lockheed Martin provides resources and an overview of the Cyber Kill Chain on their official website12.

NEW QUESTION # 108
The SOC team found a suspicious document file on a user's workstation. Upon initial inspection, the document appears benign, but deeper analysis reveals an embedded PowerShell script. The team suspects the script is designed to download and execute a malicious payload. They need to understand the script's functionality without triggering it. Which malware analysis technique is recommended to understand the PowerShell script's functionality without executing it?

- A. Dynamic analysis
- B. Static analysis
- C. Automated behavioral analysis
- D. Network traffic analysis

Answer: B

Explanation:
Static analysis is the correct approach when the requirement is to understand what the script is intended to do without executing it. For PowerShell embedded in documents, static analysis includes extracting the script content, de-obfuscating it (common techniques include base64 decoding, string reconstruction, and analyzing encoded commands), and reviewing functions, URLs/IPs, file paths, registry keys, and command-line arguments. This allows the SOC to determine likely behaviors such as downloading payloads, establishing persistence, credential theft, or disabling security controls-without risking system impact. Dynamic or behavioral analysis involves running code in a controlled sandbox to observe actions, which can be valuable but violates the constraint "without triggering it," and can be risky if containment fails or the malware has evasive logic. Network traffic analysis can help once execution has occurred or in a sandbox run, but it cannot fully explain logic that never ran. Static analysis is also useful for creating detections (hashes, strings, YARA- like patterns, command-line indicators) and for scoping across the environment by searching for matching script fragments or document markers.

NEW QUESTION # 109
Identify the event severity level in Windows logs for the events that are not necessarily significant, but may indicate a possible future problem.

- A. Warning
- B. Error
- C. Information

- D. Failure Audit

Answer: A

NEW QUESTION # 110
.....

New 312-39 Exam Online: https://www.passtestking.com/EC-COUNCIL/312-39-practice-exam-dumps.html

- EC-COUNCIL 312-39 Exam | Reliable 312-39 Cram Materials - High-quality New 312-39 Exam Online for you □ Open ➽ www.troytecdumps.com □ and search for （ 312-39 ） to download exam materials for free □Reliable 312-39 Study Plan
- Quiz 2026 312-39: The Best Reliable Certified SOC Analyst (CSA) Cram Materials □ Immediately open ➠ www.pdfvce.com □ and search for ▹ 312-39 ◃ to obtain a free download □Reliable 312-39 Study Plan
- Quiz 2026 EC-COUNCIL Perfect 312-39: Reliable Certified SOC Analyst (CSA) Cram Materials □ Enter 《 www.vce4dumps.com 》 and search for □ 312-39 □ to download for free □New 312-39 Exam Camp
- 312-39 Practice Exam □ Reliable 312-39 Study Plan □ Exam 312-39 Collection □ Search for □ 312-39 □ and download exam materials for free through ✔ www.pdfvce.com □✔□ □Reliable 312-39 Exam Practice
- New Reliable 312-39 Cram Materials | Reliable EC-COUNCIL 312-39: Certified SOC Analyst (CSA) 100% Pass □ Search for ➠ 312-39 □ and easily obtain a free download on □ www.pass4test.com □ □312-39 New Braindumps Pdf
- Quiz 2026 312-39: The Best Reliable Certified SOC Analyst (CSA) Cram Materials □ Easily obtain ➥ 312-39 □ for free download through ⇛ www.pdfvce.com ⇚ □Premium 312-39 Exam
- Exam 312-39 Collection □ 312-39 Reliable Exam Cram ↕ Premium 312-39 Exam ✏ Enter □ www.dumpsmaterials.com □ and search for （ 312-39 ） to download for free □312-39 New Braindumps Pdf
- Reliable 312-39 Exam Practice □ Premium 312-39 Exam □ Latest 312-39 Mock Exam □ Easily obtain ☀ 312-39 □☀□ for free download through 【 www.pdfvce.com 】 □Latest 312-39 Material
- Pass-Sure Reliable 312-39 Cram Materials Offer You The Best New Exam Online | Certified SOC Analyst (CSA) □ □ www.prepawaypdf.com □ is best website to obtain { 312-39 } for free download □312-39 Valid Braindumps
- EC-COUNCIL - The Best Reliable 312-39 Cram Materials □ Go to website ⇛ www.pdfvce.com ⇚ open and search for ➡ 312-39 □□□ to download for free □Reliable 312-39 Exam Practice
- Latest 312-39 Mock Exam □ 312-39 Practice Exam □ New 312-39 Exam Camp □ Search on ⇛ www.troytecdumps.com ⇚ for （ 312-39 ） to obtain exam materials for free download □312-39 Exam Preview
- yeepdirectory.com, livebackpage.com, heidimksj027729.blogripley.com, optimusbookmarks.com, mypresspage.com, wildbookmarks.com, nikolaspfxe738106.vidublog.com, ztndz.com, bookmarkindexing.com, www.stes.tyc.edu.tw, Disposable vapes

DOWNLOAD the newest PassTestking 312-39 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=10gVjF_V1oT3eWV86qfj259Njra3YMhQk