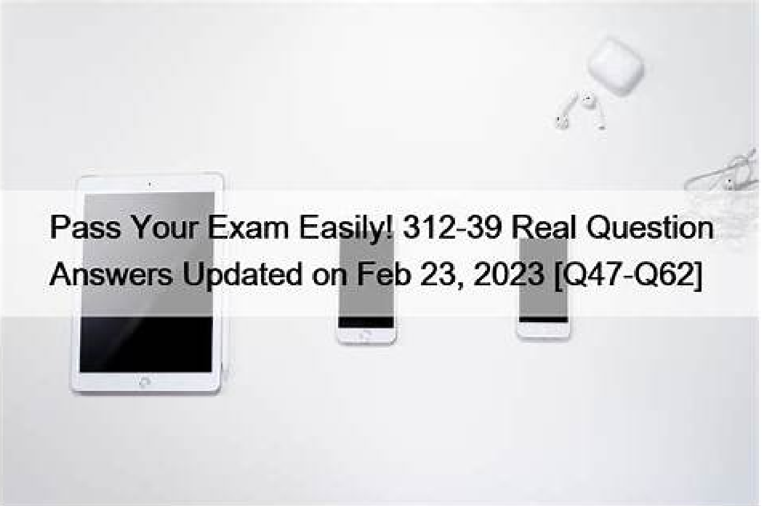
Useful Reliable 312-39 Exam Labs - Pass 312-39 Exam


Pass Your Exam Easily! 312-39 Real Question
Answers Updated on Feb 23, 2023 [Q47-Q62]

BONUS!!! Download part of TrainingDumps 312-39 dumps for free: https://drive.google.com/open?id=1xfhpCtxjYE8bGRvNTX4jPikC6rpCKnZ-

In this high-speed world, a waste of time is equal to a waste of money. As an electronic product, our 312-39 real study dumps have the distinct advantage of fast delivery. On one hand, we adopt a reasonable price for you, ensures people whoever is rich or poor would have the equal access to buy our useful 312-39 real study dumps. On the other hand, we provide you the responsible 24/7 service. Our candidates might meet so problems 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.

if you want to have a better experience on the real exam before you go to attend it, you can choose to use the software version of our 312-39 learning guide which can simulate the real exam, and you can download our 312-39 exam prep on more than one computer. We strongly believe that the software version of our 312-39 Study Materials will be of great importance for you to prepare for the exam and all of the employees in our company wish you early success.

>> Reliable 312-39 Exam Labs <<

2026 100% Free 312-39 –Perfect 100% Free Reliable Exam Labs | 312-39 Exam Torrent

We are not running around monetary objectives, customer satisfaction is our primary goal. TrainingDumps provides best after sales services, consoles the customers worries and problems through 24/7 support. Seek the appropriate guidance at TrainingDumps and get the 312-39 related help whenever you come across any problem.

To prepare for the CSA certification exam, candidates are required to have a solid understanding of cybersecurity concepts and technologies. They should also have experience working in a SOC environment and be familiar with the tools and techniques used to detect and respond to security incidents. EC-Council provides a training program to help candidates prepare for the exam. This training program covers all the topics that are included in the exam and provides hands-on experience in using the tools and techniques used by SOC analysts.

The CSA certification exam covers a wide range of topics related to security operations, including incident response, threat intelligence, network security, endpoint security, and security analytics. 312-39 Exam consists of 100 multiple-choice questions and is designed to test the learner's knowledge and expertise in the field of security operations. 312-39 exam is conducted online and can be taken from anywhere in the world, making it a convenient option for busy professionals.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q94-Q99):

NEW QUESTION # 94

John, SOC analyst wants to monitor the attempt of process creation activities from any of their Windows endpoints. Which of following Splunk query will help him to fetch related logs associated with process creation?

- A. index=windows LogName=Security EventCode=3688 NOT (Account_Name=*$) .. .. ..
- B. index=windows LogName=Security EventCode=4688 NOT (Account_Name=*$) .. .. ..
- C. index=windows LogName=Security EventCode=4678 NOT (Account_Name=*$) .. ..
- D. index=windows LogName=Security EventCode=5688 NOT (Account_Name=*$) ... ...

Answer: B

NEW QUESTION # 95
Rinni, SOC analyst, while monitoring IDS logs detected events shown in the figure below.
What does this event log indicate?

- A. XSS Attack
- B. SQL Injection Attack
- C. Directory Traversal Attack
- D. Parameter Tampering Attack

Answer: D

Explanation:
The event log indicates a ParameterTampering Attack. This type of attack involves the manipulation of parameters exchanged between the client and the server to alter application data, such as user credentials and permissions, product price and quantity, etc. The IDS log entries showing repeated access to the URL "
/OrderDetail.aspx?id=ORDR-001117" with varying order ID values suggest that the attacker is manipulating the 'id' parameter to potentially access or modify order details unauthorizedly.
References The EC-Council's Certified SOC Analyst (CSA) course materials and study guides discuss various types of cyber attacks, including Parameter Tampering, and their characteristics. Additionally, information on this type of attack can be found in resources provided by the OWASP Foundation1.
Reference: https://infosecwriteups.com/what-is-parameter-tampering-5b1beb12c5ba

NEW QUESTION # 96
A SOC analyst detects multiple instances of powershell.exe being launched with the -ExecutionPolicy Bypass and -NoProfile arguments on a domain controller. The parent process is winrm.exe, and the activity occurs during non-business hours. What should be the analyst's primary focus?

- A. Review Event ID 5145 to see if unauthorized network shares were accessed
- B. Look for Event ID 4625 to check for failed authentication attempts before execution
- C. Search for Event ID 4688 to find similar PowerShell executions within the last 24 hours
- D. Investigate Event ID 7045 to determine if a malicious service was created

Answer: C

Explanation:
The highest-signal next step is to scope and confirm the suspicious execution pattern by identifying related process creation events. Event ID 4688 records process creation in Windows Security logs when auditing is enabled, and it can capture command-line details that confirm the use of -ExecutionPolicy Bypass and - NoProfile, as well as parent/child relationships. Since the activity is on a domain controller and the parent is winrm.exe (remote management), the SOC must quickly determine whether this is isolated or part of a broader remote execution campaign. Searching for similar 4688 events over a relevant window (such as the last 24 hours) helps identify frequency, affected accounts, and whether the same command line or script path appears across hosts. Event ID 4625 (failed logon) can provide context for brute force attempts, but it does not directly validate or scope the suspicious PowerShell executions already observed. Event ID 7045 (new service installation) is important if there are signs of service-based persistence, but it is a different hypothesis. Event ID 5145 is about network share access and can be useful for lateral movement, but the immediate priority is to scope execution behavior. Therefore, focusing on 4688 process creation for similar PowerShell executions is the best primary step.

NEW QUESTION # 97

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

Answer: A

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 # 98

As a Threat Hunter at a cybersecurity company, you notice several endpoints experiencing unusual outbound traffic to an unfamiliar IP address. The traffic is encrypted and occurs in small bursts at irregular intervals.
There are no known IoCs associated with the destination, and traditional security tools have not flagged it as malicious. You decide to launch a threat-hunting initiative to determine whether this is an advanced persistent threat (APT) using sophisticated techniques to evade detection. The goal is to identify potential Indicators of Attack (IoAs) and map them against known adversary behaviors.
What type of threat hunting approach is best suited for this situation?

- A. Unstructured hunting
- B. Reactive hunting
- C. Structured hunting
- D. Situational or entity-driven hunting

Answer: A

Explanation:
Unstructured hunting is best suited when you have a weak but concerning signal (like unusual encrypted bursts to an unfamiliar IP) without a clear hypothesis tied to a known technique or indicator. In this scenario, there are no known IoCs and no alert from traditional tools, so the hunt starts from an intuition-driven anomaly and develops into hypotheses through exploration: examining which hosts are involved, what processes initiate connections, whether destinations vary, whether the behavior aligns with legitimate business tooling, and whether there are associated persistence or credential access signals. This is characteristic of unstructured hunts-analyst-driven exploration based on suspicious observations. Structured hunting typically starts with a defined hypothesis or known adversary behavior mapped to a framework and uses planned queries to confirm or refute it. Situational/entity-driven hunting focuses on a specific entity (a VIP user, crown-jewel server) or a known incident context. Reactive hunting is driven by alerts or confirmed incidents.
Here, the hunt is prompted by an anomaly without predefined IoCs or alerts, making unstructured hunting the most appropriate approach to uncover IoAs and then map findings to adversary behaviors.

NEW QUESTION # 99

......

312-39 Exam Torrent: https://www.trainingdumps.com/312-39_exam-valid-dumps.html

- 312-39 Braindumps Torrent □ 312-39 Exam Simulations □ 312-39 Latest Braindumps □ ➥ www.examdiscuss.com □ is best website to obtain ⇒ 312-39 ⇐ for free download □Valid 312-39 Test Question
- Learning Material In 3 Different Formats for EC-COUNCIL 312-39 Exam Success □ Search for □ 312-39 □ on " www.pdfvce.com " immediately to obtain a free download □Practice 312-39 Exams Free
- EC-COUNCIL 312-39 Exam Dumps For Ultimate Success 2026 □ Enter ➡ www.practicevce.com □□□ and search for 「 312-39 」 to download for free □312-39 Test Discount
- Test 312-39 Question □ Best 312-39 Study Material □ 312-39 Certified □ □ www.pdfvce.com □ is best website to obtain 【 312-39 】 for free download □312-39 Latest Braindumps
- 312-39 Latest Dumps Book □ Best 312-39 Study Material □ Best 312-39 Study Material □ Search on （ www.pdfdumps.com ） for 《 312-39 》 to obtain exam materials for free download □312-39 Detailed Study Plan
- Latest 312-39 Test Voucher □ 312-39 Real Dumps Free □ 312-39 Valid Exam Bootcamp □ Immediately open ➥ www.pdfvce.com □ and search for ⇒ 312-39 ⇐ to obtain a free download □312-39 Test Discount
- Practice 312-39 Exams Free □ 312-39 Latest Dumps Book □ 312-39 Certified □ Download ➡ 312-39 □□□ for free by simply entering ☀ www.prep4sures.top □☀□ website □Practice 312-39 Exams Free
- Learning Material In 3 Different Formats for EC-COUNCIL 312-39 Exam Success □ Search for 《 312-39 》 and download exam materials for free through ➤ www.pdfvce.com □ ↖312-39 Braindumps Torrent
- 312-39 Valid Exam Blueprint □ 312-39 Exam Simulations □ 312-39 Certified □ Simply search for " 312-39 " for free download on ▹ www.troytecdumps.com ◃ □312-39 Braindumps Torrent
- 312-39 Valid Exam Blueprint □ 312-39 Real Dumps Free □ Exam 312-39 Questions □ Search for ☀ 312-39 □☀□ and download exam materials for free through 「 www.pdfvce.com 」 □312-39 Latest Braindumps
- Learning Material In 3 Different Formats for EC-COUNCIL 312-39 Exam Success □ Easily obtain ➤ 312-39 □ for free download through ⇒ www.prepawayexam.com ⇐ □Valid 312-39 Test Question
- www.stes.tyc.edu.tw, learn.csisafety.com.au, www.stes.tyc.edu.tw, 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, learningskill.site, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

2026 Latest TrainingDumps 312-39 PDF Dumps and 312-39 Exam Engine Free Share: https://drive.google.com/open?id=1xfhpCtxjYE8bGRvNTX4jPikC6rpCKnZ-