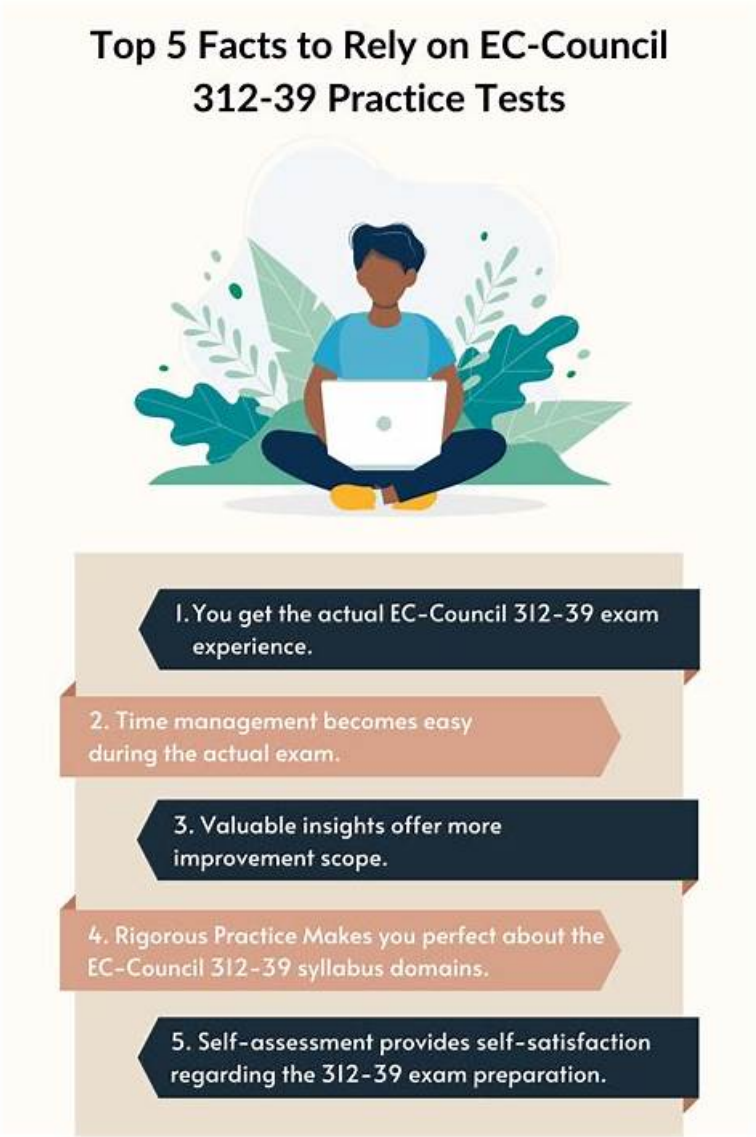
Study 312-39 Reference, Reliable 312-39 Test Camp



What's more, part of that BraindumpsPass 312-39 dumps now are free: https://drive.google.com/open?id=1w8iyS8V3TZ3jFMGT8RKwPqyXjkYXV6x3

What was your original intention of choosing a product? I believe that you must have something you want to get. 312-39 exam materials allow you to have greater protection on your dreams. This is due to the high passing rate of our 312-39 study questions which is high as 98% to 100%. And our 312-39 exam questions own a high quality which is easy to understand and practice. At the same time, our price is charming. Just come and buy it!

To be eligible for the exam, candidates must have at least two years of experience in the field of information security and must have completed an EC-COUNCIL training program or an equivalent course. 312-39 Exam consists of 100 multiple-choice questions, and candidates must score at least 70% to pass. 312-39 exam is available online and can be taken from anywhere in the world.

>> Study 312-39 Reference <<

Reliable EC-COUNCIL 312-39 Test Camp & Valid 312-39 Exam Syllabus

Our clients come from all around the world and our company sends the products to them quickly. The clients only need to choose the version of the product, fill in the correct mails and pay for our Certified SOC Analyst (CSA) guide dump. Then they will receive our mails in 5-10 minutes. Once the clients click on the links they can use our 312-39 Study Materials immediately. If the clients

can’t receive the mails they can contact our online customer service and they will help them solve the problem. Finally the clients will receive the mails successfully. The purchase procedures are simple and the delivery of our 312-39 study tool is fast.

The EC-Council 312-39 Exam covers a wide range of topics related to cybersecurity, including threat intelligence, network security, incident response, and risk management. 312-39 exam is designed to test the candidate's ability to identify and analyze security threats, as well as their ability to respond to those threats in a way that minimizes the impact on the organization. Successful completion of the exam demonstrates that the individual has the knowledge and skills necessary to effectively perform the role of a SOC analyst and contribute to the overall security posture of an organization.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q93-Q98):

NEW QUESTION # 93
A multinational financial institution notices unusual network activity during a routine security audit. The SOC detects multiple failed login attempts, followed by a successful access attempt using an administrator's credentials from an unrecognized IP address. Shortly after, sensitive customer records are accessed without authorization. The company suspects a breach and calls in the forensic investigation team. During evidence collection, the forensic team creates a detailed record that tracks every individual who handled the evidence, its storage location, and timestamps of transfers. What is this process called?

- A. Incident Documentation
- B. Digital Fingerprinting
- C. Chain of Custody
- D. Data Imaging

Answer: C

Explanation:
Chain of custody is the formal process used to document and preserve evidence integrity by recording who collected the evidence, who accessed it, where it was stored, and when it changed hands. In SOC and forensic operations, chain of custody is essential for maintaining evidentiary reliability, especially in cases with regulatory, legal, or disciplinary implications. It ensures that evidence has not been altered, tampered with, or mishandled, and it supports defensible conclusions about what occurred. Incident documentation is broader and includes timelines, decisions, actions taken, and communications, but it does not specifically track evidence handling transfers. Data imaging is the creation of a forensic copy of storage media (disk image), a separate technical step that may be recorded within chain-of-custody logs. Digital fingerprinting refers to generating hashes or other identifiers to confirm file integrity; again, it is a technique used within evidence handling, but the tracking record of handlers, locations, and transfers is chain of custody. For SOC analysts, correctly maintaining chain of custody is critical when responding to breaches involving sensitive customer records and potential compliance investigations.

NEW QUESTION # 94
Which of the following event detection techniques uses User and Entity Behavior Analytics (UEBA)?

- A. Rule-based detection
- B. Heuristic-based detection
- C. Signature-based detection
- D. Anomaly-based detection

Answer: D

Explanation:
User and Entity Behavior Analytics (UEBA) is a cybersecurity process that uses machine learning, algorithms, and statistical analyses to detect abnormal behavior of users and entities within an organization. UEBA systems analyze patterns of behavior and can identify anomalies that deviate from the norm, which could indicate a potential security threat.
Anomaly-based detection is the technique that aligns with UEBA's functionality. It contrasts with:
* Rule-based detection, which relies on predefined rules to detect threats.
* Heuristic-based detection, which uses experience-based techniques.
* Signature-based detection, which depends on known patterns or signatures of malware to identify threats.
Anomaly-based detection systems are designed to be dynamic, continuously learning and establishing what is considered normal to identify deviations. This approach is particularly effective in identifying previously unknown threats, hence its alignment with UEBA.
References: The EC-Council's Certified SOC Analyst (CSA) program covers the fundamentals of SOC operations, including incident detection with Security Information and Event Management (SIEM) and enhanced incident detection with Threat Intelligence, which encompasses the use of UEBA for anomaly detection123.

NEW QUESTION # 95
An attacker exploits the logic validation mechanisms of an e-commerce website. He successfully purchases a product worth $100 for $10 by modifying the URL exchanged between the client and the server.
Original
URL: http://www.buyonline.com/product.aspx?profile=12
&debit=100
Modified URL: http://www.buyonline.com/product.aspx?profile=12
&debit=10
Identify the attack depicted in the above scenario.

- A. Session Fixation Attack
- B. SQL Injection Attack
- C. Denial-of-Service Attack
- D. Parameter Tampering Attack

Answer: D

Explanation:
The scenario described involves an attacker modifying the URL parameters to alter the price of a product, which is a classic example of a Parameter Tampering attack. This type of attack occurs when an attacker manipulates parameters exchanged between client and server in order to modify application data, such as user credentials, permissions, and price of products, as seen in this case.
The original URL indicates that the product price (debit) is set to $100. The attacker has modified this parameter value to $10 in the modified URL, thus exploiting the logic validation mechanism of the e-commerce website to purchase the product at a lower price.
This manipulation of parameters is indicative of a Parameter Tampering attack, which is a form of web-based attack where the properties of a web application are altered to achieve unintended outcomes by the attacker.
References: The EC-Council's Certified SOC Analyst (CSA) course material covers various types of cyber attacks, including Parameter Tampering. The CSA study guides and resources provide detailed information on how to identify and respond to such attacks, emphasizing the importance of validating and sanitizing all inputs and parameters to prevent exploitation.

NEW QUESTION # 96
Rinni, SOC analyst, while monitoring IDS logs detected events shown in the figure below.
What does this event log indicate?

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

Answer: D

NEW QUESTION # 97
Which of the following factors determine the choice of SIEM architecture?

- A. Network Topology
- B. DHCP Configuration
- C. DNS Configuration
- D. SMTP Configuration

Answer: A

Explanation:

NEW QUESTION # 98
.....

Reliable 312-39 Test Camp: https://www.braindumpspass.com/EC-COUNCIL/312-39-practice-exam-dumps.html

- 100% Pass Quiz EC-COUNCIL - Trustable 312-39 - Study Certified SOC Analyst (CSA) Reference □ Open website ▹ www.easy4engine.com ◃ and search for { 312-39 } for free download □312-39 Actualtest
- Useful Study 312-39 Reference – Find Shortcut to Pass 312-39 Exam □ Immediately open ▹ www.pdfvce.com ◃ and search for ✔ 312-39 □✔□ to obtain a free download □Relevant 312-39 Answers
- Useful Study 312-39 Reference – Find Shortcut to Pass 312-39 Exam □□ The page for free download of □ 312-39 □ on [www.examcollectionpass.com] will open immediately □Test 312-39 Score Report
- Book 312-39 Free □ 312-39 Learning Engine □ 312-39 Valid Braindumps Free □ Easily obtain " 312-39 " for free download through " www.pdfvce.com " □312-39 Latest Test Prep
- 312-39 Valid Test Discount □ 312-39 Exams Dumps □ Valid 312-39 Test Duration □ The page for free download of ▸ 312-39 ◂ on ▹ www.practicevce.com ◃ will open immediately □Valid Dumps 312-39 Book
- Valid 312-39 Test Duration □ 312-39 Learning Engine □ Valid 312-39 Exam Pattern □ Open website □ www.pdfvce.com □ and search for ▸ 312-39 ◂ for free download □312-39 Learning Engine
- Quiz EC-COUNCIL - The Best 312-39 - Study Certified SOC Analyst (CSA) Reference □ Immediately open ➥ www.troytecdumps.com □ and search for ▹ 312-39 ◃ to obtain a free download □Latest 312-39 Dumps Book
- Pass Guaranteed 2026 Accurate EC-COUNCIL 312-39: Study Certified SOC Analyst (CSA) Reference □ Enter { www.pdfvce.com } and search for 「 312-39 」 to download for free □312-39 Actual Tests
- EC-COUNCIL 312-39 Exam Dumps - A Surefire Way To Achieve Success □ 「 www.examcollectionpass.com 」 is best website to obtain □ 312-39 □ for free download □312-39 Valid Test Discount
- Test 312-39 Score Report □ Test 312-39 Score Report □ 312-39 Exam Questions And Answers □ Search for □ 312-39 □ and download it for free on ▹ www.pdfvce.com ◃ website □312-39 Learning Engine
- 2026 100% Free 312-39 –Newest 100% Free Study Reference | Reliable Certified SOC Analyst (CSA) Test Camp □ Enter " www.troytecdumps.com " and search for □ 312-39 □ to download for free □Valid 312-39 Exam Pattern
- myportal.utt.edu.tt, gettr.com, www.xiaodingdong.store, thecodingtracker.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, www.stes.tyc.edu.tw, www.dkcomposite.com, notefolio.net, 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, Disposable vapes

P.S. Free & New 312-39 dumps are available on Google Drive shared by BraindumpsPass: https://drive.google.com/open?id=1w8iyS8V3TZ3jFMGT8RKwPqyXjkYXV6x3