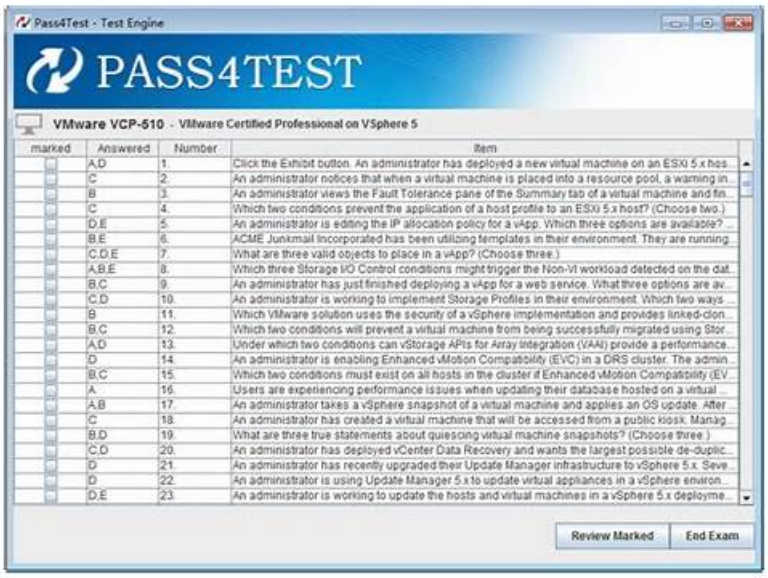
312-39 Study Materials & 312-39 VCE Dumps & 312-39 Test Prep



BONUS!!! Download part of PremiumVCEDump 312-39 dumps for free: https://drive.google.com/open?id=1kTDUW5Q6sRXDMvNibNFv9JGBXcSxSHN7

Our 312-39 test prep is renowned for free renewal in the whole year. As you have experienced various kinds of exams, you must have realized that renewal is invaluable to 312-39 study materials, especially to such important 312-39 exams. And there is no doubt that being acquainted with the latest trend of exams will, to a considerable extent, act as a driving force for you to pass the exams and realize your dream of living a totally different life. So if you do want to achieve your dream, buy our 312-39 practice materials.

The EC-COUNCIL 312-39 Exam covers a range of topics related to SOC analysis, including network security and threat analysis, incident response and management, and security operations center processes and procedures. Candidates will be expected to demonstrate their knowledge and skills in these areas through a combination of multiple-choice questions, scenario-based questions, and hands-on simulations.

>> Valid 312-39 Exam Labs <<

Pass Guaranteed Quiz EC-COUNCIL - Updated Valid 312-39 Exam Labs

Our company committed all versions of 312-39 practice materials attached with free update service. When 312-39 exam preparation has new updates, the customer services staff will send you the latest version. So we never stop the pace of offering the best services and 312-39 practice materials for you. And we offer you the free demo of our 312-39 Learning Materials to check the quality before payment. Tens of thousands of candidates have fostered learning abilities by using our 312-39 Learning materials you can be one of them definitely.

EC-COUNCIL 312-39: Certified SOC Analyst (CSA) Exam is a globally recognized certification that demonstrates an individual's knowledge and skills in detecting, investigating, and responding to security incidents. It is an excellent certification for IT professionals who wish to advance their careers in the cybersecurity industry or for those who work in Security Operations Centers (SOCs). Passing the exam requires a comprehensive understanding of network security, threat intelligence, incident response, and compliance.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q154-Q159):

NEW QUESTION # 154
Which of the following formula is used to calculate the EPS of the organization?

- A. EPS = number of security events / time in seconds
- B. EPS = number of correlated events / time in seconds

- C. EPS = number of normalized events / time in seconds
- D. EPS = average number of correlated events / time in seconds

Answer: B

Explanation:
In the context of a Security Operations Center (SOC), EPS typically refers to "Events Per Second," which is a measure of the number of security events processed in one second. The correct formula for calculating EPS in a SOC environment is the number of correlated events divided by the time in seconds. Correlated events are those that have been analyzed and aggregated by the SOC's security information and event management (SIEM) system, indicating a potential security incident. This metric helps in understanding the operational load and performance of the SOC.
References: The information is aligned with the EC-Council's Certified SOC Analyst (CSA) course material and best practices, which emphasize the importance of understanding and managing SOC operational metrics such as EPS for effective security monitoring and incident response12.

NEW QUESTION # 155
TechSolutions, a software development firm, discovered a potential data leak after an external security researcher reported finding sensitive customer data on a public code repository. Level 1 SOC analysts confirmed the presence of the data and escalated the issue. Level 2 analysts traced the source of the leak to an internal network account. The incident response team has been alerted, and the CISO demands a comprehensive analysis of the incident, including the extent of the data breach and the timeline of events. The SOC manager must decide whom to assign to the in-depth investigation. To accurately determine the timeline, extent, and root cause of the data leak, which SOC role is critical in gathering and analyzing digital evidence?

- A. Subject Matter Expert
- B. Forensic Analyst
- C. SOC Manager
- D. Threat Intelligence Analyst

Answer: B

Explanation:
A forensic analyst is the role best suited to perform in-depth evidence gathering and analysis required to reconstruct timelines, determine scope, and establish root cause for a data leak. This work includes preserving evidence (ensuring integrity), collecting endpoint and server artifacts, reviewing authentication and repository access logs, correlating commit history with identity and device telemetry, and building a defensible chain of events for leadership and potential legal/regulatory review. The SOC manager coordinates resources and priorities but typically does not perform hands-on forensic reconstruction. A subject matter expert may provide domain expertise (e.g., on Git workflows, cloud platforms, or database systems), but forensic rigor and evidence handling are the core requirement here. A threat intelligence analyst focuses on external adversary information, campaigns, and indicators; they can assist with context but are not the primary role for internal evidence reconstruction. Because the CISO needs timeline, extent, and root cause-deliverables that depend on digital evidence handling and forensic methodology-the forensic analyst is the critical assignment.

NEW QUESTION # 156
Which attack works like a dictionary attack, but adds some numbers and symbols to the words from the dictionary and tries to crack the password?

- A. Rainbow Table Attack
- B. Hybrid Attack
- C. Bruteforce Attack
- D. Birthday Attack

Answer: C

NEW QUESTION # 157
Which of the following service provides phishing protection and content filtering to manage the Internet experience on and off your network with the acceptable use or compliance policies?

- A. Malstrom

- B. I-Blocklist
- C. Apility.io
- D. OpenDNS

Answer: D

Explanation:
OpenDNS provides extensive phishing protection and content filtering services. It operates by enforcing internet use policies on and off the network, ensuring that users adhere to acceptable use and compliance policies. Here's how OpenDNS achieves this:
* Phishing Protection: OpenDNS uses predictive security to anticipate and prevent threats before they can reach the network. It does this by using DNS to enforce security, which is often quicker and more effective than traditional methods.
* Content Filtering: OpenDNS allows the network administrator to block unwanted content categories, thus enforcing compliance with organizational policies. This is done through DNS queries, which are checked against OpenDNS's database to ensure they comply with the set policies.
* Off-Network Protection: OpenDNS's roaming client allows the same level of protection and filtering even when devices are not connected to the company network, ensuring consistent enforcement of policies.
References:
* EC-Council's Certified SOC Analyst (C|SA) program provides training and certification for SOC analysts, covering the fundamentals of SOC operations, including phishing protection and content filtering 1.
* Additional resources and study guides from the EC-Council elaborate on the role of SOC analysts and the tools they use, including services like OpenDNS for maintaining network security and integrity 23.

NEW QUESTION # 158
Which of the following is a correct flow of the stages in an incident handling and response (IH&R) process?

- A. Incident Recording -> Preparation -> Containment -> Incident Triage -> Recovery -> Eradication -> Post-Incident Activities
- B. Incident Triage -> Eradication -> Containment -> Incident Recording -> Preparation -> Recovery -> Post-Incident Activities
- C. Preparation -> Incident Recording -> Incident Triage -> Containment -> Eradication -> Recovery -> Post-Incident Activities
- D. Containment -> Incident Recording -> Incident Triage -> Preparation -> Recovery -> Eradication -> Post-Incident Activities

Answer: C

Explanation:
The correct flow of stages in an Incident Handling and Response (IH&R) process typically follows a structured approach that begins with Preparation, which is crucial for an effective response to incidents. This is followed by Incident Recording, where details of the incident are documented. Incident Triage is the next stage, where incidents are prioritized based on their impact. Containment strategies are then employed to limit the spread of the incident. Eradication involves removing the threat from the affected systems. Recovery is the process of restoring systems to normal operation. Finally, Post-Incident Activities involve learning from the incident and improving future response efforts.
References: The stages of the IH&R process are outlined in various EC-Council resources, including the EC-Council's Certified Incident Handler (E|CIH) program and related training materials, which emphasize the importance of a structured and methodical approach to incident handling and response123.

NEW QUESTION # 159
.....

- Quiz EC-COUNCIL Pass-Sure 312-39 - Valid Certified SOC Analyst (CSA) Exam Labs □ Immediately open □ www.pdfvce.com □ and search for ▹ 312-39 ◃ to obtain a free download □312-39 Exam Tests
- Pass Guaranteed Quiz 2026 EC-COUNCIL 312-39: Accurate Valid Certified SOC Analyst (CSA) Exam Labs □ Search for □ 312-39 □ and download it for free immediately on ☀ www.vce4dumps.com □☀□ □Test 312-39 Free
- Hot 312-39 Spot Questions □ Reliable 312-39 Test Materials □ Latest Test 312-39 Simulations □ Download ➽ 312-39 □ for free by simply searching on 【 www.pdfvce.com 】 □Study 312-39 Center
- 312-39 100% Accuracy □ Reliable 312-39 Test Review □ Latest Test 312-39 Simulations □ Search for [312-39] and easily obtain a free download on ➤ www.troytecdumps.com □ □312-39 Latest Study Plan
- New Released EC-COUNCIL 312-39 Questions Verified by Experts [2026] □ Download ➠ 312-39 □ for free by simply entering ➤ www.pdfvce.com □ website □Study 312-39 Center
- Quiz Fantastic 312-39 - Valid Certified SOC Analyst (CSA) Exam Labs □ Immediately open ☀ www.prepawayete.com □☀□ and search for 「 312-39 」 to obtain a free download □New 312-39 Study Guide
- 312-39 Latest Study Plan □ Latest Test 312-39 Simulations □ Pdf 312-39 Torrent □ Enter ▹ www.pdfvce.com ◃ and search for ➤ 312-39 □ to download for free □Latest Test 312-39 Simulations
- 2026 Latest 312-39 – 100% Free Valid Exam Labs | 312-39 Relevant Exam Dumps □ Search for ➽ 312-39 □ and download exam materials for free through { www.vce4dumps.com } □Exam Dumps 312-39 Free
- startupxplore.com, englishprep.sarvanimmigration.ca, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, bd.enrollbusiness.com, quay.io, 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 PremiumVCEDump 312-39 dumps for free: https://drive.google.com/open?id=1kTDUW5Q6sRXDMvNibNFv9JGBXcSxSHN7