Pass Guaranteed Quiz EC-COUNCIL - 312-39 - Certified SOC Analyst (CSA) Accurate Test Objectives Pdf

BTW, DOWNLOAD part of TestkingPass 312-39 dumps from Cloud Storage: https://drive.google.com/open?id=1lCKbfwF1JNddTJLWzVp3UMrVzjKGyrwK

Nowadays, computers develop rapidly, and it makes our daily life and work more convenient. IT workers positions are popular in 21th century. EC-COUNCIL 312-39 exam questions are also known by many IT certification candidates. If candidates can get a golden certification, senior positions with high salary and good benefits are waiting for you. Our latest and Valid 312-39 Exam Questions may be the best helper for candidates working for EC-COUNCIL certifications.

About the upcoming 312-39 exam, do you have mastered the key parts which the exam will test up to now? Everyone is conscious of the importance and only the smart one with smart way can make it. When new changes or knowledge are updated, our experts add additive content into our 312-39 latest material. They have always been in a trend of advancement. Admittedly, our 312-39 Real Questions are your best choice. We also estimate the following trend of exam questions may appear in the next exam according to syllabus. So they are the newest and also the most trustworthy 312-39 exam prep to obtain.

>> 312-39 Test Objectives Pdf <<

312-39 online test engine & 312-39 training study & 312-39 torrent dumps

TestkingPass's study material is available in three different formats. The reason we have introduced three formats of the Certified SOC Analyst (CSA) (312-39) practice material is to meet the learning needs of every student. Some candidates prefer 312-39 practice exams and some want Real 312-39 Questions due to a shortage of time. At TestkingPass, we meet the needs of both types of aspirants. We have EC-COUNCIL 312-39 PDF format, a web-based practice exam, and Certified SOC Analyst (CSA) (312-39) desktop practice test software.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q150-Q155):

NEW QUESTION # 150
What does Windows event ID 4740 indicate?

- A. A user account was disabled.
- B. A user account was created.
- C. A user account wasenabled.
- D. A user account was locked out.

Answer: D

Explanation:
Event ID 4740 is a security audit event in Windows that indicates a user account has been locked out. This event is generated every time the system locks out a user account due to repeated logon failures, which are typically caused by incorrect password entries. The event is logged on domain controllers, member servers, and workstations where the lockout occurred. It includes details such as the account name, domain, and the computer from which the lockout originated.
References: The information is verified as per Microsoft's official documentation and learning resources related to security auditing and user account management. Specifically, the Microsoft Learn page on security auditing provides comprehensive details on Event ID 47401. Additionally, resources like Ultimate Windows Security offer in-depth explanations of this event and its implications for security monitoring2.
Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4740#:~:text=For%204740(S)%3A%20A,Security%20ID'%20is%20not%20SYSTEM.

NEW QUESTION # 151
Which of the following framework describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering?

- A. COBIT
- B. ITIL
- C. SSE-CMM
- D. SOC-CMM

Answer: C

Explanation:
The Systems Security Engineering Capability Maturity Model (SSE-CMM) is the framework that describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering. The SSE-CMM provides a standard metric for security engineering practices, covering the entire lifecycle of development, operation, maintenance, and decommissioning activities. It also includes management, organizational, and engineering activities, as well as interactions with other disciplines and organizations1.
References: The ISO/IEC 21827:2008 standard specifies the SSE-CMM and outlines its role in defining the essential characteristics of an organization's security engineering process1. This standard is recognized and used as a reference for good security engineering practices within the industry.
Reference: https://www.iso.org/standard/44716.html

NEW QUESTION # 152
Banter is a threat analyst in Christine Group of Industries. As a part ofthe job, he is currently formatting and structuring the raw data. He is at which stage of the threat intelligence life cycle?

- A. Collection
- B. Dissemination and Integration
- C. Analysis and Production
- D. Processing and Exploitation

Answer: D

Explanation:
In thethreat intelligence life cycle, the stage of Processing and Exploitation involves the formatting and structuring of raw data. This is the phase where collected data is turned into a format that can be more easily analyzed and used. Banter, as a threat analyst, is engaged in this specific activity, which indicates that he is in the Processing and Exploitation stage. This stage is crucial as it prepares the data for further analysis and production of actionable intelligence.
References: The EC-Council's Certified Threat Intelligence Analyst (C|TIA) program outlines the threat intelligence life cycle and defines the Processing and Exploitation stage as the point where data is organized and prepared for analysis. This information is

detailed in the EC-Council's official training and certification resources for the SOC Analyst role12.
Reference: https://socradar.io/5-stages-of-the-threat-intelligence-lifecycle/

NEW QUESTION # 153
Jane, a security analyst, while analyzing IDS logs, detected an event matching Regex
/((\%3C)|<)((\%69)|i|(\% 49))((\%6D)|m|(\%4D))((\%67)|g|(\%47))[