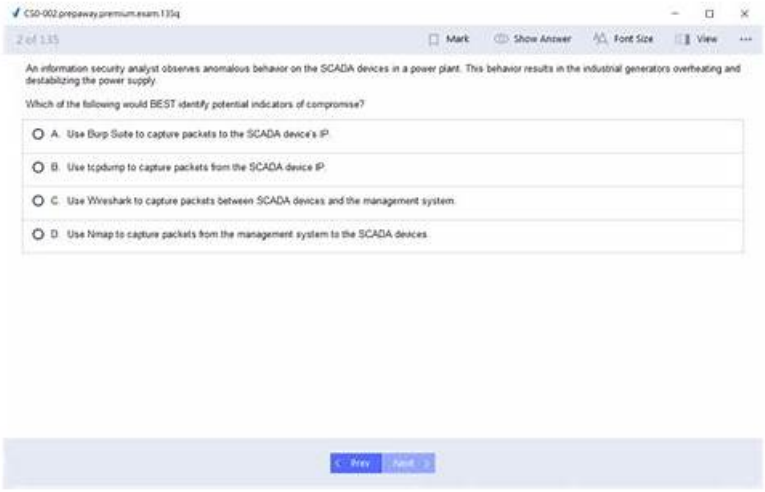
Updated CS0-002 Prepaway Dumps Spend Your Little Time and Energy to Clear CompTIA CS0-002: CompTIA Cybersecurity Analyst (CySA+) Certification Exam exam



What's more, part of that Actualtests4sure CS0-002 dumps now are free: https://drive.google.com/open?id=1EU24bjS5a2pDpDu2QqbgUhBus8YvllIk

With the development of science, our life has become more and more comfortable and convenient than ever before. CompTIA certifications are attractive and CS0-002 exam learning materials become popular since IT workers positions are much in demand. Technology change world. There are many opportunities in the internet every day. Ambitious people may choose CS0-002 Exam Learning materials into internet area and want to do something different.

Our product boosts many merits and useful functions to make you to learn efficiently and easily. Our CS0-002 guide questions are compiled and approved elaborately by experienced professionals and experts. The download and tryout of our CS0-002 torrent question before the purchase are free and we provide free update and the discounts to the old client. Our customer service personnel are working on the whole day and can solve your doubts and questions at any time. Our online purchase procedures are safe and carry no viruses so you can download, install and use our CS0-002 Guide Torrent safely.

>> CS0-002 Prepaway Dumps <<

CompTIA CS0-002 PDF Dumps Format - A Convenient Preparation Method

Although a lot of products are cheap, but the quality is poor, perhaps users have the same concern for our CS0-002 learning materials. Here, we solemnly promise to users that our product error rate is zero. Everything that appears in our products has been inspected by experts. In our CS0-002 learning material, users will not even find a small error, such as spelling errors or grammatical errors. It is believed that no one is willing to buy defective products, so, the CS0-002 study materials have established a strict quality control system.

The CySA+ certification exam covers a wide range of cybersecurity topics, including threat and vulnerability management, incident response, security architecture and toolsets, and compliance and governance. Candidates will also be tested on their ability to analyze and interpret data to identify security risks and develop strategies to mitigate them.

CompTIA Cybersecurity Analyst (CySA+) Certification Exam Sample Questions (Q57-Q62):

NEW QUESTION # 57
A small business does not have enough staff in the accounting department to segregate duties. The controller writes the checks for the business and reconciles them against the ledger. To ensure there is no fraud occurring, the business conducts quarterly reviews in which a different officer in the business compares all the cleared checks against the ledger. Which of the following BEST describes this type of control?

- A. Preventive
- B. Compensating
- C. Detective
- D. Deterrent

Answer: B

Explanation:
A compensating control, also called an alternative control, is a mechanism that is put in place to satisfy the requirement for a security measure that is deemed too difficult or impractical to implement at the present time.
"Compensating controls are additional security measures that you take to address a vulnerability without remediating the underlying issue." A compensating control is a control that reduces the risk of an existing or potential control weakness2 In this case, the lack of segregation of duties in the accounting department is a control weakness that increases the risk of fraud or error. The quarterly reviews by a different officer are a compensating control that reduces this risk by providing an independent verification of the transactions recorded by the controller.

NEW QUESTION # 58
A developer wrote a script to make names and other PII data unidentifiable before loading a database export into the testing system Which of the following describes the type of control that is being used?

- A. Data encoding
- B. Data masking
- C. Data loss prevention
- D. Data classification

Answer: C

NEW QUESTION # 59
During routine monitoring a security analyst identified the following enterprise network traffic:
Packet capture output:
Which of the following BEST describes what the security analyst observed?

- A. 192.168.12.21 made a TCP connection to 66 187 224 210
- B. 192.168.12.21 made a TCP connection to 209 132 177 50
- C. 66.187.224.210 set up a DNS hijack with 192.168.12.21.
- D. 209.132.177.50 set up a TCP reset attack to 192 168 12 21

Answer: B

NEW QUESTION # 60
A company's Chief Information Security Officer (CISO) is concerned about the integrity of some highly confidential files. Any changes to these files must be tied back to a specific authorized user's activity session. Which of the following is the BEST technique to address the CISO's concerns?

- A. Place a legal hold on the files. Require authorized users to abide by a strict time context access policy. Monitor the files for unauthorized changes.
- B. Use Wireshark to scan all traffic to and from the directory. Monitor the files for unauthorized changes.
- C. Regularly use SHA-256 to hash the directory containing the sensitive information. Monitor the files for unauthorized changes.
- D. Configure DLP to reject all changes to the files without pre-authorization. Monitor the files for unauthorized changes.

Answer: A,D

NEW QUESTION # 61
Approximately 100 employees at your company have received a phishing email. As a security analyst you have been tasked with handling this situation.

INSTRUCTIONS
Review the information provided and determine the following:
1. How many employees clicked on the link in the phishing email?
2. On how many workstations was the malware installed?
3. What is the executable file name or the malware?

Answer:

Explanation:
see the explanation.
Explanation
Select the following answer as per diagram below.

NEW QUESTION # 62
.....

CompTIA CS0-002 is one of the important certification exams. Actualtests4sure's experienced IT experts through their extensive experience and professional IT expertise have come up with IT certification exam study materials to help people pass CompTIA Certification CS0-002 Exam successfully. Actualtests4sure's providing learning materials can not only help you 100% pass the exam, but also provide you a free one-year update service.