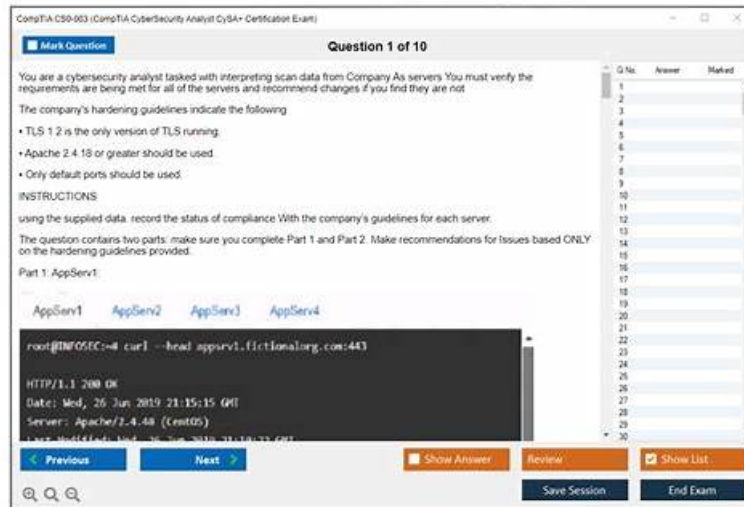


# CompTIA CS0-003 Latest Braindumps Sheet & Customizable CS0-003 Exam Mode



P.S. Free 2026 CompTIA CS0-003 dumps are available on Google Drive shared by PassCollection: [https://drive.google.com/open?id=1GLa44pWC195aexjGNOjd98zQsdO\\_-GO6](https://drive.google.com/open?id=1GLa44pWC195aexjGNOjd98zQsdO_-GO6)

The PassCollection is a reliable and trusted platform for quick and complete CompTIA CS0-003 exam preparation. At this platform, you can easily download real and verified CompTIA Cybersecurity Analyst (CySA+) Certification Exam (CS0-003) exam practice questions. These CompTIA Cybersecurity Analyst (CySA+) Certification Exam (CS0-003) exam questions are ideal and recommended study material for quick and complete CompTIA CS0-003 exam preparation.

CompTIA Cybersecurity Analyst (CySA+) Certification is recognized by employers worldwide and is in high demand. CompTIA Cybersecurity Analyst (CySA+) Certification Exam certification demonstrates that the candidate has the skills and knowledge to protect against cybersecurity threats and incidents. CompTIA Cybersecurity Analyst (CySA+) Certification Exam certification is ideal for professionals who are looking to advance their careers in cybersecurity and want to demonstrate their expertise in this field.

>> **CompTIA CS0-003 Latest Braindumps Sheet** <<

## Customizable CS0-003 Exam Mode & Reliable CS0-003 Braindumps

Did you often feel helpless and confused during the preparation of the exam? Do you want to find an expert to help but feel bad about the expensive tutoring costs? Don't worry. CS0-003 learning materials can help you to solve all the problems. CS0-003 learning material always regards helping students to pass the exam as it is own mission. With CS0-003 learning materials, you only need to pay half the money to get the help of the most authoritative experts.

## CompTIA Cybersecurity Analyst (CySA+) Certification Exam Sample Questions (Q620-Q625):

### NEW QUESTION # 620

A SOC manager is looking for a solution that can improve the response time and execute predetermined instructions. Which of the following is the best solution based on these requirements?

- **A. SOAR**
- B. XDR
- C. CASB
- D. SIEM

**Answer: A**

Explanation:

SOAR (Security Orchestration, Automation, and Response) platforms are designed to automate response actions and execute predetermined instructions, significantly improving incident response times for security operations teams.

#### NEW QUESTION # 621

A Chief Information Security Officer (CISO) has determined through lessons learned and an associated after-action report that staff members who use legacy applications do not adequately understand how to differentiate between non-malicious emails and phishing emails. Which of the following should the CISO include in an action plan to remediate this issue?

- A. Awareness training and education
- B. Multifactor authentication on all systems
- C. Replacement of legacy applications
- D. Organizational governance

**Answer: A**

Explanation:

Awareness training and education are essential to help staff recognize phishing emails and understand safe email practices, particularly when using legacy applications that might not have the latest security features. Training helps build a culture of security mindfulness, which is critical for preventing social engineering attacks. According to CompTIA Security+ and CySA+ frameworks, user education is a fundamental aspect of organizational defense against phishing. Options like replacing applications or implementing MFA (while helpful) do not directly address the need for user awareness in this scenario.

#### NEW QUESTION # 622

An IT professional is reviewing the output from the top command in Linux. In this company, only IT and security staff are allowed to have elevated privileges. Both departments have confirmed they are not working on anything that requires elevated privileges. Based on the output below:

```
PID
USER
VIRT
RES
SHR
%CPU
%MEM
TIME+
COMMAND
34834
person
4980644
224288
111076
5.3
14.44
1:41.44
cinnamon
34218
person
51052
30920
23828
4.7
0.2
0:26.54
Xorg
2264
root
449628
143500
26372
```

14.0  
3.1  
0:12.38  
bash  
35963  
xrdp  
711940  
42356  
10560  
2.0  
0.2  
0:06.81  
xrdp

Which of the following PIDs is most likely to contribute to data exfiltration?

- A. 0
- B. 1
- C. 2
- **D. 3**

**Answer: D**

Explanation:

\* PID 2264 (bash running as root) is suspicious because:

\* It has elevated privileges (root user).

\* Bash (command-line shell) is running with high CPU usage (14.0%), which is unusual unless actively being used.

\* If unauthorized, an attacker could be exfiltrating data via command-line methods like scp, wget, or custom scripts.

Why Not Other Options?

\* B (34218 - Xorg) # Xorg is a display server for GUI; no signs of exfiltration.

\* C (34834 - Cinnamon) # Cinnamon is a desktop environment, not a threat.

\* D (35963 - xrdp) # xrdp is a remote desktop service, expected behavior.

### NEW QUESTION # 623

During a scan of a web server in the perimeter network, a vulnerability was identified that could be exploited over port 3389. The web server is protected by a WAF. Which of the following best represents the change to overall risk associated with this vulnerability?

- A. The risk would decrease because a web application firewall is in place
- B. The risk would decrease because RDP is blocked by the firewall
- **C. The risk would increase because the host is external facing**
- D. The risk would not change because network firewalls are in use

**Answer: C**

### NEW QUESTION # 624

Which of the following best explains the importance of playbooks for incident response teams?

- A. Playbooks help implement mitigation controls to prevent the occurrence of incidents in accordance with internal policies and procedures as designed by the IT team.
- B. Playbooks set baseline requirements that are implemented before incidents happen to ensure the proper monitoring process in order to collect metrics and KPIs that will be used for lessons- learned procedures after a postmortem analysis.
- **C. Playbooks help minimize negative impacts and restore data, systems, and operations through highly detailed, preplanned procedures that will be followed when particular types of incidents occur.**
- D. Playbooks define compliance controls and help keep the monitoring process that is in place fully aligned with regulatory requirements as designed by international rules.

**Answer: C**

Explanation:

- What's more, part of that PassCollection CS0-003 dumps now are free: [https://drive.google.com/open?id=1GLa44pWC195aexjGNOjd98zQsdO\\_-GO6](https://drive.google.com/open?id=1GLa44pWC195aexjGNOjd98zQsdO_-GO6)