

# Free PDF Quiz CompTIA - Useful CS0-003 Study Materials Review

**STUDY4**  
exam

**CompTIA**  
CS0-003 Exam

CompTIA CyberSecurity Analyst CySA+ Certification Exam

QUESTIONS & ANSWERS  
**DEMO VERSION**  
(LIMITED CONTENT)

Thank you for Downloading CS0-003 exam PDF Demo

You can also try our CS0-003 practice exam software

Download Free Demo

<http://www.study4exam.com/CS0-003.html>

BONUS!!! Download part of Prep4away CS0-003 dumps for free: <https://drive.google.com/open?id=1vQbVbvfMHXprEWRPdbSOF1dGzCUATA2d>

Prep4away is a good website for CompTIA certification CS0-003 exams to provide short-term effective training. And Prep4away can guarantee your CompTIA certification CS0-003 exam to be qualified. If you don't pass the exam, we will take a full refund to you. Before you choose to buy the Prep4away products before, you can free download part of the exercises and answers about CompTIA Certification CS0-003 Exam as a try, then you will be more confident to choose Prep4away's products to prepare your CompTIA certification CS0-003 exam.

To pass the CS0-003 Certification Exam, candidates must demonstrate their ability to perform real-world cybersecurity tasks. They must be able to analyze data to identify security threats, develop and implement effective security policies and procedures, and respond to security incidents in a timely and effective manner. Candidates are expected to have a strong understanding of cybersecurity concepts and principles, as well as hands-on experience in the field.

>> CS0-003 Study Materials Review <<

**CompTIA Cybersecurity Analyst (CySA+) Certification Exam exam training dumps & CS0-003 free latest pdf & CompTIA Cybersecurity Analyst**

## (CySA+) Certification Exam latest torrent vce

You can enjoy the instant download of CS0-003 exam dumps after purchase so you can start studying with no time wasted. You can install our CS0-003 study file on your computer or other device as you like without any doubts. Because our CS0-003 test engine is virus-free, you can rest assured to use. What's more, the CS0-003 Questions and answers are the best valid and latest, which can ensure 100% pass. Our 24/7 customer service is available and you can contact us for any questions about CompTIA practice dumps.

## CompTIA Cybersecurity Analyst (CySA+) Certification Exam Sample Questions (Q534-Q539):

### NEW QUESTION # 534

A team of analysts is developing a new internal system that correlates information from a variety of sources, analyzes that information, and then triggers notifications according to company policy.

Which of the following technologies was deployed?

- A. CERT
- B. SIEM
- C. IPS
- D. SOAR

**Answer: B**

### NEW QUESTION # 535

An organization's website was maliciously altered.

#### INSTRUCTIONS

Review information in each tab to select the source IP the analyst should be concerned about, the indicator of compromise, and the two appropriate corrective actions.

SFTP log   Netstat   HTTP access

```
2022-04-01 16:04:12 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 192.168.10.32] [username = sjames]
2022-04-01 16:04:33 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022-04-01 16:05:30 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./about_us.html written]
2022-04-01 16:09:20 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 192.168.10.32] [username = sjames]
2022-04-01 17:10:42 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 192.168.10.37] [username = sjames]
2022-04-01 17:11:30 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022-04-01 17:14:30 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./index written]
2022-04-01 17:15:44 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 192.168.10.37] [username = sjames]
2022-04-01 19:45:48 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 32.111.16.37] [username = sjames]
2022-04-01 19:45:58 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 32.111.16.37] [username = sjames]
2022-04-01 23:01:50 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 41.21.18.102] [username = sjames]
2022-04-01 23:01:54 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022-04-01 23:02:25 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./index.html written]
2022-04-01 23:03:18 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 41.21.18.102] [username = sjames]
2022-04-01 23:35:28 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (failed login) [IP = 32.111.16.37] [username = sjames]
2022-04-02 09:10:42 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 192.168.11.102] [username = sjames]
2022-04-02 09:15:44 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022-04-02 09:22:55 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./index written]
2022-04-02 09:23:12 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 192.168.11.102] [username = sjames]
```

**Which source IP address should the analyst be most concerned about:**

Select

**Identify the indicator of compromise:**

CompTIA

**Select the corrective actions:**

- Encrypt index.html.
- Change the password on the sjames account.
- Block external sftp access.
- Shut down the insecure file transfer server.
- Delete the sjames account.
- Deny 192.168.\*.\* at firewall.

SFTP log

Netstat

HTTP access

CompTIA

```

2022-04-01 16:04:12 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 192.168.10.32] [username = sjames]
2022-04-01 16:04:33 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022-04-01 16:05:30 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./about_us.html written]
2022-04-01 16:09:20 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 192.168.10.32] [username = sjames]
2022-04-01 17:10:42 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 192.168.10.37] [username = sjames]
2022-04-01 17:11:30 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022-04-01 17:14:30 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./index written]
2022-04-01 17:15:44 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 192.168.10.37] [username = sjames]
2022-04-01 19:45:48 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 32.111.16.37] [username = sjames]
2022-04-01 19:45:58 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 32.111.16.37] [username = sjames]
2022-04-01 23:01:50 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 41.21.18.102] [username = sjames]
2022-04-01 23:01:54 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022-04-01 23:02:25 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./index.html written]
2022-04-01 23:03:18 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 41.21.18.102] [username = sjames]
2022-04-01 23:35:28 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (failed login) [IP = 32.111.16.37] [username = sjames]
2022-04-02 09:10:42 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 192.168.11.102] [username = sjames]
2022-04-02 09:15:44 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022-04-02 09:22:55 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./index written]
2022-04-02 09:23:12 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 192.168.11.102] [username = sjames]

```

Which source IP address should the analyst be most concerned about:

Select

- 41.21.18.102
- 192.168.11.102
- 192.168.10.37
- 52.110.26.27
- 192.168.10.32
- 32.111.16.37

Select the corrective actions:

- Encrypt index.html.
- Change the password on the sjames account.
- Block external sftp access.
- Shut down the insecure file transfer server.
- Delete the sjames account.
- Deny 192.168.\*.\* at firewall.

Identify the indicator of compromise:

Select

- 404 server error
- Modified index.html file
- Unauthorized username
- Modified about\_us file
- Repeated failed logins
- Select

SFTP log

Netstat

HTTP access

```

> netstat -ano
TCP 0.0.0.0:22 0.0.0.0:0 LISTENING 1600
TCP 127.0.0.1:1960 127.0.0.1:49722 ESTABLISHED 1000
TCP 127.0.0.1:1960 127.0.0.1:49022 ESTABLISHED 1000
TCP 127.0.0.1:49722 127.0.0.1:1960 ESTABLISHED 4912
TCP 127.0.0.1:49800 127.0.0.1:1960 ESTABLISHED 4228
TCP 127.0.0.1:49801 127.0.0.1:1961 ESTABLISHED 4228
TCP 127.0.0.1:38666 41.21.18.102:22 ESTABLISHED 4940
TCP 127.0.0.1:55356 192.168.10.32:22 ESTABLISHED 5112
TCP 127.0.0.1:37654 192.168.10.37:22 ESTABLISHED 5104
TCP 127.0.0.1:55357 32.111.16.37:22 TIME_WAIT 0
TCP 127.0.0.1:52744 32.111.16.37:22 TIME_WAIT 0
TCP 127.0.0.1:56751 32.111.16.37:22 TIME_WAIT 0
TCP 127.0.0.1:39882 104.17.18.29:22 SYN_SENT 4992

```

SFTP log	Netstat	HTTP access
192.168.10.32	- "" -	[2022-04-01 16:05:45 "GET https://mycompany.com/about_us.html" HTTP/1.1 200]
192.168.10.37	- "" -	[2022-04-01 17:15:20 "GET https://mycompany.com" HTTP/1.1 200]
107.31.28.112	- "" -	[2022-04-01 22:11:56 "GET https://mycompany.com" HTTP/1.1 200]
63.11.108.122	- "" -	[2022-04-01 22:22:58 "GET https://mycompany.com" HTTP/1.1 200]
41.21.18.102	- "" -	[2022-04-01 23:02:56 "GET https://mycompany.com" HTTP/1.1 200]
32.111.16.37	- "" -	[2022-04-01 23:34:01 "GET https://mycompany.com" HTTP/1.1 200]
52.110.26.27	- "" -	[2022-04-01 23:35:08 "GET https://mycompany.com/aboutUs.html" HTTP/1.1 404]
52.110.26.27	- "" -	[2022-04-01 23:35:18 "GET https://mycompany.com/aboutUs.html" HTTP/1.1 404]
52.110.26.27	- "" -	[2022-04-01 23:35:22 "GET https://mycompany.com/aboutUs.html" HTTP/1.1 404]
192.168.11.102	- "" -	[2022-04-02 09:23:02 "GET https://mycompany.com" HTTP/1.1 200]
63.11.108.122	- "" -	[2022-04-02 10:12:18 "GET https://mycompany.com" HTTP/1.1 200]
63.11.108.122	- "" -	[2022-04-02 10:12:28 "GET https://mycompany.com/about_us" HTTP/1.1 200]

**Answer:**

**Explanation:**

see the explanation for step by step solution.

**Explanation:**

**Step 1: Analyzing the SFTP Log**

The SFTP log provides a record of file transfer and login activities:

- \* User "sjames" logged in from several IP addresses:
- \* 192.168.10.32 and 192.168.10.37 (internal network IPs)
- \* 32.111.16.37 and 41.21.18.102 (external IPs)
- \* We see file alterations in the /var/www directory, which is commonly the web directory.
- \* Modified files: about\_us.html, index.html
- \* Suspicious activity:
- \* 192.168.11.102 and 41.21.18.102 modified the files.
- \* 32.111.16.37 had failed login attempts, indicating possible unauthorized access attempts.

The most suspicious IP here is 41.21.18.102, as it's associated with direct file modifications, possibly indicating unauthorized access.

**Step 2: Reviewing Netstat**

The netstat output shows active connections and their states:

- \* IP 41.21.18.102 has an ESTABLISHED connection with port 22, commonly used for SFTP.
- \* IP 32.111.16.37 is also attempting connections, and 32.111.16.37 connections are in a TIME\_WAIT state, showing prior connections were recently closed.

The netstat output reaffirms 41.21.18.102 is actively connected and potentially involved in malicious activities.

**Step 3: Checking the HTTP Access Log**

The HTTP Access log shows access to about\_us.html:

- \* 32.111.16.37 repeatedly accessed /about\_us.html with 404 errors, indicating attempts to reach non-existing pages.
- \* 41.21.18.102 accessed the 200 status code, showing successful page requests, but since this IP was modifying files directly on the server, it might be testing or verifying changes.

Again, 41.21.18.102 stands out as it matches both successful file modification and page request patterns, while 32.111.16.37 shows unsuccessful attempts.

**Step 4: Selecting the IP of Concern**

Based on the above analysis:

- \* answer: 41.21.18.102 should be the IP of concern due to its direct file modifications on critical web files (about\_us.html, index.html).

**Step 5: Identifying the Indicator of Compromise**

Potential indicators include unauthorized file modifications:

- \* Modified index.html file is the correct answer, as it indicates direct changes to website content and is often a clear sign of compromise.

**Step 6: Selecting Corrective Actions**

To mitigate and prevent further compromise:

- \* Change the password on the "sjames" account: The account was used across various IPs, indicating potential account compromise.
- \* Block external SFTP access: Restricting SFTP to internal IPs only would prevent unauthorized external modifications. Since 41.21.18.102 was external, this would stop similar threats.

**Summary**

- \* IP of Concern: 41.21.18.102
- \* Indicator of Compromise: Modified index.html file
- \* Corrective Actions:
  - \* Change the password on the sjames account
  - \* Block external SFTP access

These selections address both the immediate security breach and implement a preventative measure against future unauthorized access.

SFTP log	Netstat	HTTP access
<pre> 192.168.10.32 - "" - [2022-04-01 16:05:45 "GET https://mycompany.com/about_us.html" HTTP/1.1 200] 192.168.10.37 - "" - [2022-04-01 17:15:20 "GET https://mycompany.com" HTTP/1.1 200] 107.31.28.112 - "" - [2022-04-01 22:11:56 "GET https://mycompany.com" HTTP/1.1 200] 63.11.108.122 - "" - [2022-04-01 22:22:58 "GET https://mycompany.com" HTTP/1.1 200] 41.21.18.102 - "" - [2022-04-01 23:02:56 "GET https://mycompany.com" HTTP/1.1 200] 32.111.16.37 - "" - [2022-04-01 23:34:01 "GET https://mycompany.com" HTTP/1.1 200] 52.110.26.27 - "" - [2022-04-01 23:35:08 "GET https://mycompany.com/aboutUs.html" HTTP/1.1 404] 52.110.26.27 - "" - [2022-04-01 23:35:18 "GET https://mycompany.com/aboutUs.html" HTTP/1.1 404] 52.110.26.27 - "" - [2022-04-01 23:35:22 "GET https://mycompany.com/aboutUs.html" HTTP/1.1 404] 192.168.11.102 - "" - [2022-04-02 09:23:02 "GET http://mycompany.com" HTTP/1.1 200] 63.11.108.122 - "" - [2022-04-02 10:12:18 "GET https://mycompany.com" HTTP/1.1 200] 63.11.108.122 - "" - [2022-04-02 10:12:28 "GET https://mycompany.com/about_us" HTTP/1.1 200]           </pre>		
<p>Which source IP address should the analyst be most concerned about:</p> <p>41.21.18.102</p>		<p>Select the corrective actions:</p> <p><input type="checkbox"/> Shut down the insecure file transfer server.</p> <p><input type="checkbox"/> Encrypt index.html.</p> <p><input checked="" type="checkbox"/> Change the password on the sjames account.</p> <p><input type="checkbox"/> Deny 192.168.*.* at firewall.</p> <p><input checked="" type="checkbox"/> Block external sftp access.</p> <p><input type="checkbox"/> Delete the sjames account.</p>
<p>Identify the indicator of compromise:</p> <p>Modified index.html file</p>		

### NEW QUESTION # 536

During an incident involving phishing, a security analyst needs to find the source of the malicious email. Which of the following techniques would provide the analyst with this information?

- A. SSL inspection
- B. Packet capture
- C. Reverse engineering
- **D. Header analysis**

**Answer: D**

Explanation:

Header analysis is the technique of examining the metadata of an email, such as the sender, recipient, date, subject, and routing information. It can help to identify the source of a malicious email by revealing the IP address and domain name of the originator, as well as any spoofing or redirection attempts. References:

CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 6, page 240; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 6, page 249.

### NEW QUESTION # 537

After an upgrade to a new EDR, a security analyst received reports that several endpoints were not communicating with the SaaS provider to receive critical threat signatures. To comply with the incident response playbook, the security analyst was required to validate connectivity to ensure communications. The security analyst ran a command that provided the following output:

ComputerName: comptia007

RemotePort: 443

InterfaceAlias: Ethernet 3

TcpTestSucceeded: False

Which of the following did the analyst use to ensure connectivity?

- A. nmap
- **B. tnc**
- C. tracert
- D. ping

**Answer: B**

Explanation:

Comprehensive Detailed

The command output shown indicates that the analyst used a TCP connection test to check if communication on port 443 (usually HTTPS) succeeded. Here's why each option was or was not suitable:

- A . nmap: While nmap can scan ports, it does not provide direct feedback on connection success or failure in the manner shown.
- B . tnc (Test-NetConnection in PowerShell): This command in PowerShell is specifically designed to test connectivity to a specified port and IP address. The output (TcpTestSucceeded: False) is characteristic of the tnc command.
- C . ping: The ping command only tests ICMP echo replies and does not indicate success or failure on specific ports.
- D . tracert: tracert traces the path packets take to reach a host but does not provide a direct indication of port availability or success.

Reference:

Microsoft PowerShell Documentation: Test-NetConnection cmdlet, which details TCP port testing.

NIST SP 800-115: Technical Guide to Information Security Testing and Assessment, covering connectivity testing methods.

### NEW QUESTION # 538

During a tabletop exercise, engineers discovered that an ICS could not be updated due to hardware versioning incompatibility. Which of the following is the most likely cause of this issue?

- **A. Legacy system**
- B. Configuration management
- C. Degrading functionality
- D. Business process interruption

**Answer: A**

Explanation:

The most likely cause of the issue where an ICS (Industrial Control System) could not be updated due to hardware versioning incompatibility is a legacy system. Legacy systems often have outdated hardware and software that may not be compatible with modern updates and patches. This can pose significant challenges in maintaining security and operational efficiency.

### NEW QUESTION # 539

.....

People always tend to neglect the great power of accumulation, thus the CS0-003 study materials can not only benefit one's learning process but also help people develop a good habit of preventing delays. We have full confidence to ensure that you will have an enjoyable study experience with our CS0-003 Study Materials, which are designed to arouse your interest and help you pass the exam more easily. You will have a better understanding after reading the following advantages.

**Examcollection CS0-003 Vce:** <https://www.prep4away.com/CompTIA-certification/braindumps.CS0-003.ete.file.html>

- Examcollection CS0-003 Free Dumps  CS0-003 New Braindumps Free  CS0-003 Valid Dumps Files  Search for **▶ CS0-003 ◀** on ( [www.verifieddumps.com](http://www.verifieddumps.com) ) immediately to obtain a free download  CS0-003 New Braindumps Free
- CS0-003 Test Questions Vce  New CS0-003 Dumps  New CS0-003 Test Experience  Enter  [www.pdfvce.com](http://www.pdfvce.com)  and search for { CS0-003 } to download for free  CS0-003 Examinations Actual Questions
- Pass Guaranteed Quiz 2026 CompTIA The Best CS0-003: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Study Materials Review  The page for free download of  CS0-003   on  on  ⇒ [www.testkingpass.com](http://www.testkingpass.com) ⇐ will open immediately  Valid CS0-003 Test Review
- Pass Guaranteed Quiz 2026 The Best CompTIA CS0-003 Study Materials Review  Open website  [www.pdfvce.com](http://www.pdfvce.com)  and search for **▶ CS0-003**  for free download  CS0-003 New Braindumps Free
- New CS0-003 Dumps  CS0-003 Certification Questions  Examcollection CS0-003 Free Dumps  **▶** [www.troytecdumps.com](http://www.troytecdumps.com)  is best website to obtain  CS0-003   for free download  CS0-003 Valid Torrent
- CS0-003 Updated Test Cram  CS0-003 New Braindumps Free  CS0-003 New Dumps Ppt  Open (

