



# CS0-002<sup>Q&As</sup>

CompTIA Cybersecurity Analyst (CySA+)

## Pass CompTIA CS0-002 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/cs0-002.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA  
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 1**

A security analyst has been alerted to several emails that show evidence an employee is planning malicious activities that involve employee PII on the network before leaving the organization. The security analysis BEST response would be to coordinate with the legal department and:

- A. the public relations department
- B. senior leadership
- C. law enforcement
- D. the human resources department

Correct Answer: D

---

**QUESTION 2**

A web developer wants to create a new web part within the company website that aggregates sales from individual team sites. A cybersecurity analyst wants to ensure security measurements are implemented during this process. Which of the following remediation actions should the analyst take to implement a vulnerability management process?

- A. Personnel training
- B. Vulnerability scan
- C. Change management
- D. Sandboxing

Correct Answer: C

---

**QUESTION 3**

An analyst received a forensically sound copy of an employee's hard drive. The employee's manager suspects inappropriate images may have been deleted from the hard drive. Which of the following could help the analyst recover the deleted evidence?

- A. File hashing utility
- B. File timestamps
- C. File carving tool
- D. File analysis tool

Correct Answer: C

---

**QUESTION 4**



A system's authority to operate (ATO) is set to expire in four days. Because of other activities and limited staffing, the organization has neglected to start reauthentication activities until now. The cybersecurity group just performed a vulnerability scan with the partial set of results shown below:

```
-----
Scan Host: 192.168.1.13
15-Jan-16 08:12:10.1 EDT

Vulnerability CVE-2015-1635
HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8,
Windows 8.1 and Windows Server 2012 allows remote attackers to execute
arbitrary code via crafted HTTP requests, aka "HTTP.sys remote code execution
vulnerability"

Severity: 10.0 (high)

Expected Result: enforceHTTPValidation='enabled';
Current Value: enforceHTTPValidation=enabled;

Evidence:
C:\%system%\Windows\config\web.config
-----
```

Based on the scenario and the output from the vulnerability scan, which of the following should the security team do with this finding?

- A. Remediate by going to the web config file, searching for the enforce HTTP validation setting, and manually updating to the correct setting.
- B. Accept this risk for now because this is a "high" severity, but testing will require more than the four days available, and the system ATO needs to be completed.
- C. Ignore it. This is false positive, and the organization needs to focus its efforts on other findings.
- D. Ensure HTTP validation is enabled by rebooting the server.

Correct Answer: A

---

## QUESTION 5

An international company is implementing a marketing campaign for a new product and needs a security analyst to perform a threat-hunting process to identify possible threat actors. Which of the following should be the analyst's primary focus?

- A. Hacktivists
- B. Organized crime
- C. Nation-states
- D. Insider threats

Correct Answer: B



VCE & PDF

Pass4itSure.com

<https://www.pass4itsure.com/cs0-002.html>

2024 Latest pass4itsure CS0-002 PDF and VCE dumps Download

---

[Latest CS0-002 Dumps](#)

[CS0-002 PDF Dumps](#)

[CS0-002 Braindumps](#)