

Test CompTIA CS0-002 Cram Review, CS0-002 Reliable Exam Price



DOWNLOAD the newest Real4dumps CS0-002 PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=1htS20XmFLFSUJrNB6brbz7EqbaMRcn0V>

In addition to the content updates, our system will also be updated for the CS0-002 training materials. If you have any opinions, you can tell us that our common goal is to create a product that users are satisfied with. After you start learning, I hope you can set a fixed time to check emails. If the content of the CS0-002 Practice Guide or system is updated, we will send updated information to your e-mail address. Of course, you can also consult our e-mail on the status of the product updates. I hope we can work together to make you better use CS0-002 simulating exam to pass the CS0-002 exam.

CompTIA CySA+ certification is ideal for IT professionals who want to specialize in cybersecurity and advance their careers in this field. CompTIA Cybersecurity Analyst (CySA+) Certification Exam certification is recognized globally and is an excellent way to demonstrate your expertise and knowledge to potential employers. With the increasing number of cyber threats and attacks, organizations are looking for skilled professionals who can protect their systems and data from potential threats, making the CompTIA CySA+ certification an in-demand credential in the cybersecurity industry.

>> Test CompTIA CS0-002 Cram Review <<

CS0-002 Reliable Exam Price & Valid CS0-002 Test Camp

These CompTIA CS0-002 exam questions are modeled after the CS0-002 test. They will assist you in learning how to manage your time during the examination. Real4dumps enabled all users to regulate time during their CompTIA Cybersecurity Analyst (CySA+) Certification Exam CS0-002 test. And it can be accomplished via practice, as practice makes perfect. Therefore, you must practice passing the CS0-002 exam.

CompTIA Cybersecurity Analyst (CySA+) Certification Exam Sample Questions (Q116-Q121):

NEW QUESTION # 116

Which of the following BEST describes what an organization's incident response plan should cover regarding how the organization handles public or private disclosures of an incident?

- A. The disclosure section should focus on how to reduce the likelihood customers will leave due to the incident.
- B. The disclosure section should include the names and contact information of key employees who are needed for incident resolution.
- C. The disclosure section should contain language explaining how the organization will reduce the likelihood of the incident from happening in the future.
- **D. The disclosure section should contain the organization's legal and regulatory requirements regarding disclosures.**

Answer: D

Explanation:

The disclosure section of an organization's incident response plan should cover how the organization handles public or private disclosures of an incident. The disclosure section should contain the organization's legal and regulatory requirements regarding disclosures, such as the type, content, format, timing, and recipients of the disclosures. The disclosure section should also specify the roles and responsibilities of the personnel involved in the disclosure process, such as who is authorized to make or approve disclosures, who is responsible for communicating with internal and external stakeholders, and who is accountable for ensuring compliance with the disclosure requirements. The disclosure section should not focus on how to reduce the likelihood customers will leave due to the incident (A), as this is a business objective rather than a disclosure requirement. The disclosure section should not include the names and contact information of key employees who are needed for incident resolution, as this is an operational detail rather than a disclosure requirement. The disclosure section should not contain language explaining how the organization will reduce the likelihood of the incident from happening in the future (D), as this is a remediation action rather than a disclosure requirement.

NEW QUESTION # 117

A user's computer has been running slowly when the user tries to access web pages. A security analyst runs the command `netstat -aon` from the command line and receives the following output:

Which of the following lines indicates the computer may be compromised?

- A. Line 4
- **B. Line 3**
- C. Line 6
- D. Line 5
- E. Line 2
- F. Line 1

Answer: B

NEW QUESTION # 118

Organizational policies require vulnerability remediation on severity 7 or greater within one week.

Anything with a severity less than 7 must be remediated within 30 days. The organization also requires security teams to investigate the details of a vulnerability before performing any remediation. If the investigation determines the finding is a false positive, no remediation is performed and the vulnerability scanner configuration is updated to omit the false positive from future scans:

The organization has three Apache web servers:

The results of a recent vulnerability scan are shown below:

The team performs some investigation and finds a statement from Apache:

Which of the following actions should the security team perform?

- A. Investigate the false negative on 192.168.1.20
- **B. Remediate 192.168.1.22 within 30 days**
- C. Ignore the false positive on 192.168.1.22
- D. Remediate 192.168.1.20 within 30 days

Answer: B

NEW QUESTION # 119

An organization has a strict policy that if elevated permissions are needed, users should always run commands under their own account, with temporary administrator privileges if necessary. A security analyst is reviewing syslog entries and sees the following:

Which of the following entries should cause the analyst the MOST concern?

- A. `<100>2 2020-01-10T20:36:36.0010z financeserver su 201 32001 = BOM ' sudo vi users.txt success`
- **B. `<100>2 2020-01-10T19:33:41.002z webserver su 201 32001 = BOM ' su vi httpd.conf failed for joe`**
- C. `<100> 2020-01-10T19:34.002z financeserver su 201 32001 = BOM ' su vi success`
- D. `<100> 2020-01-10T19:33:48.002z webserver sudo 201 32001 = BOM ' su vi httpd.conf success`
- E. `<100> 2020-01-10T19:33:48.002z webserver sudo 201 32001 = BOM ' su vi syslog.conf failed for jos`

Answer: B

