# High-quality CS0-002 Exam Tips Supply you Authorized Trustworthy Source for CS0-002: CompTIA Cybersecurity Analyst (CySA+) Certification Exam to Prepare casually


What's more, part of that ITPassLeader CS0-002 dumps now are free: https://drive.google.com/open?id=1Di9EG27Hp7mOr35lE2UubH2YJDU0B_8h

our company made our CS0-002 practice guide with accountability. Our CS0-002 training dumps are made by our CS0-002 exam questions responsible company which means you can gain many other benefits as well. We offer free demos of our for your reference, and send you the new updates if our experts make them freely. What is more, we give some favorable discount on our CS0-002 Study Materials from time to time, which mean that you can have more preferable price to buy our products.

CompTIA Cybersecurity Analyst (CySA+) certification exam, also known as the CS0-002 Exam, is a globally recognized certification that validates the skills required to perform the duties of a cybersecurity analyst. It is designed to test the knowledge of cybersecurity professionals in the areas of threat management, vulnerability management, incident response, and security architecture and toolsets.

**>> CS0-002 Exam Tips <<**

## Precise CS0-002 Exam Questions offer you high-efficient Study Materials - ITPassLeader

Are you planning to attempt the CompTIA CS0-002 exam of the CS0-002 certification? The first hurdle you face while preparing for the CompTIA Cybersecurity Analyst (CySA+) Certification Exam (CS0-002) exam is not finding the trusted brand of accurate and updated CS0-002 exam questions. If you don't want to face this issue then you are at the trusted spot. ITPassLeader is offering actual and Latest CS0-002 Exam Questions that ensure your success in the CompTIA CS0-002 certification exam on your maiden attempt.

## CompTIA Cybersecurity Analyst (CySA+) Certification Exam Sample

## Questions (Q147-Q152):

**NEW QUESTION # 147**
A security analyst for a large pharmaceutical company was given credentials from a threat intelligence resources organisation for Internal users, which contain usernames and valid passwords for company accounts.
Which of the following is the FIRST action the analyst should take as part of security operations monitoring?

- A. Run scheduled antivirus scans on all employees' machines to look for malicious processes.
- B. Reimage the machines of all users within the group in case of a malware infection.
- C. Search the event logs for event identifiers that indicate Mimikatz was used.
- D. Change all the user passwords to ensure the malicious actors cannot use them.

**Answer: C**

**NEW QUESTION # 148**
While conducting a cloud assessment, a security analyst performs a Prowler scan, which generates the following within the report:
Based on the Prowler report, which of the following is the BEST recommendation?

- A. Delete BusinessUsr access key 1.
- B. Delete access key 2.
- C. Delete CloudDev access key 1.
- D. Delete access key 1.

**Answer: D**

Explanation:
Prowler is a tool that can scan AWS environments for security issues and compliance violations. The Prowler report shows that there are two access keys for CloudDev user: access key 1 and access key 2. Access key 1 has not been used in more than 90 days, which violates the AWS CIS benchmark 1.4 (Ensure access keys are rotated every 90 days or less). Therefore, the best recommendation is to delete access key 1 and use access key 2 instead. Deleting CloudDev access key 1, deleting BusinessUsr access key 1, or deleting access key 2 are not appropriate recommendations based on the Prowler report. Reference: https://github.com/toniblyx/prowler

**NEW QUESTION # 149**
An analyst is performing a BIA and needs to consider measures and metrics. Which of the following would help the analyst achieve this objective? (Select two).

- A. Time to reimage the server
- B. Time required to inform stakeholders about outage
- C. Maximum downtime before impact is unacceptable
- D. Minimum data backup volume
- E. Disaster recovery plan for non-critical services
- F. Total time accepted for business process outage

**Answer: C,F**

Explanation:
The objective of a BIA is to determine the potential impacts of various disruptions on the business processes and functions, and to establish the recovery priorities and objectives for each process and function. To achieve this objective, the analyst needs to consider various measures and metrics that can quantify the impacts and the recovery requirements. Some of the common measures and metrics that are used in a BIA are:
Maximum downtime before impact is unacceptable: This metric defines the maximum amount of time that a business process or function can be disrupted without causing significant or irreversible damage to the organization's reputation, operations, finances, or legal obligations. This metric is also known as the maximum tolerable downtime (MTD) or maximum tolerable period of disruption (MTPD). It helps to determine the recovery time objective (RTO), which is the target time for restoring the process or function to an acceptable level of service after a disruption1.
Total time accepted for business process outage: This metric defines the total amount of time that a business process or function can be out of service within a given period, such as a day, a week, or a month. This metric is also known as the recovery point objective (RPO), which is the maximum amount of data loss or corruption that can be tolerated after a disruption1. It helps to determine the

backup frequency and retention policy for the data and systems that support the process or function.
Time required to inform stakeholders about outage: This metric defines the time frame for communicating with the internal and external stakeholders who are affected by or involved in the disruption and recovery of a business process or function. This metric helps to establish the crisis communication plan and protocol, which specifies who, what, when, where, why, and how to communicate during and after a disruption2. It also helps to manage the expectations and perceptions of the stakeholders and to maintain their trust and confidence in the organization.
Time to reimage the server: This metric defines the time needed to restore a server to its original or desired state after a disruption. This metric helps to estimate the resources and efforts required for recovering the server and its applications. It also helps to evaluate the feasibility and effectiveness of different recovery strategies, such as restoring from backup, rebuilding from scratch, or replacing with a spare3.
Minimum data backup volume: This metric defines the minimum amount of data that needs to be backed up regularly to ensure the continuity and integrity of a business process or function. This metric helps to optimize the backup process and reduce the storage costs and bandwidth consumption. It also helps to identify the critical data elements and sources that are essential for the process or function4.

**NEW QUESTION # 150**
While analyzing logs from a WAF, a cybersecurity analyst finds the following:
Which of the following BEST describes what the analyst has found?

- A. This is an encrypted packet
- B. A packet is being used to bypass the WAF
- C. This is an encrypted GET HTTP request
- D. This is an encoded WAF bypass

**Answer: D**

**NEW QUESTION # 151**
In order to meet regulatory compliance objectives for the storage of PHI, vulnerability scans must be conducted on a continuous basis.
The last completed scan of the network returned 5,682 possible vulnerabilities.
The Chief Information Officer (CIO) would like to establish a remediation plan to resolve all known issues.
Which of the following is the BEST way to proceed?

- A. Place assets that handle PHI in a sandbox environment, and then resolve all vulnerabilities.
- B. Attempt to identify all false positives and exceptions, and then resolve all remaining items.
- C. Reduce the scan to items identified as critical in the asset inventory, and resolve these issues first.
- D. Hold off on additional scanning until the current list of vulnerabilities have been resolved.

**Answer: C**

**NEW QUESTION # 152**
.....

Our CS0-002 exam preparation materials are the hard-won fruit of our experts with their unswerving efforts in designing products and choosing test questions. Pass rate is what we care for preparing for an examination, which is the final goal of our CS0-002 certification guide. According to the feedback of our users, we have the pass rate of 99%, which is equal to 100% in some sense. The high quality of our products also embodies in its short-time learning. You are only supposed to practice CS0-002 Guide Torrent for about 20 to 30 hours before you are fully equipped to take part in the examination.

➥ www.easy4engine.com □ website □New CS0-002 Study Guide

- CS0-002 Actual Real Exam - CS0-002 Test Questions - CS0-002 Dumps Torrent □ Enter 「 www.pdfvce.com 」 and search for { CS0-002 } to download for free □CS0-002 Practice Exam Online
- CS0-002 Practice Exam Online □ Simulations CS0-002 Pdf □ Latest CS0-002 Test Labs □ Easily obtain { CS0-002 } for free download through ➡ www.prepawaypdf.com □□□ □Latest CS0-002 Material
- CS0-002 Vce Files □ Simulations CS0-002 Pdf □ Exam CS0-002 Tutorial □ Search for ⇛ CS0-002 ⇚ and obtain a free download on " www.pdfvce.com " □Premium CS0-002 Exam
- Latest CS0-002 Exam Preparation □ CS0-002 Answers Free □ Valid CS0-002 Exam Sims □ Simply search for □ CS0-002 □ for free download on ✔ www.dumpsmaterials.com □✔□ □CS0-002 Answers Free
- Excellent CS0-002 Exam Tips - 100% Pass CS0-002 Exam □ Enter ➥ www.pdfvce.com □ and search for ⇛ CS0-002 ⇚ to download for free □Latest CS0-002 Exam Preparation
- Premium CS0-002 Exam □ Latest CS0-002 Exam Preparation □ CS0-002 Cert □ Enter ➥ www.pdfdumps.com □ □ and search for ⇛ CS0-002 ⇚ to download for free □Latest CS0-002 Material
- Premium CS0-002 Exam □ CS0-002 Answers Free □ New CS0-002 Study Guide □ Search on □ www.pdfvce.com □ for ➤ CS0-002 □ to obtain exam materials for free download □Exam CS0-002 Tutorial
- CS0-002 Vce Files □ CS0-002 Guaranteed Success □ Latest CS0-002 Test Labs □ The page for free download of ➽ CS0-002 □ on （ www.validtorrent.com ） will open immediately □Latest CS0-002 Braindumps Free
- bookmark-media.com, franceshsgc548216.verybigblog.com, aoifefmcj797955.blog2freedom.com, thebookpage.com, hannalwrq151780.aboutyoublog.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, delilahdjog403091.bloggosite.com, tasneemboym463393.plpwiki.com, sparxsocial.com, Disposable vapes

P.S. Free 2026 CompTIA CS0-002 dumps are available on Google Drive shared by ITPassLeader: https://drive.google.com/open?id=1Di9EG27Hp7mOr35lE2UubH2YJDU0B_8h