



RC0-C02^{Q&As}

CompTIA Advanced Security Practitioner (CASP) Recertification Exam
for Continuing Education

Pass CompTIA RC0-C02 Exam with 100% Guarantee

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

<https://www.pass4itsure.com/rc0-c02.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 forensic analyst receives a hard drive containing malware quarantined by the antivirus application. After creating an image and determining the directory location of the malware file, which of the following helps to determine when the system became infected?

- A. The malware file's modify, access, change time properties.
- B. The timeline analysis of the file system.
- C. The time stamp of the malware in the swap file.
- D. The date/time stamp of the malware detection in the antivirus logs.

Correct Answer: B

Timelines can be used in digital forensics to identify when activity occurred on a computer. Timelines are mainly used for data reduction or identifying specific state changes that have occurred on a computer.

QUESTION 2

A security engineer is working on a large software development project. As part of the design of the project, various stakeholder requirements were gathered and decomposed to an implementable and testable level. Various security requirements were also documented.

Organize the following security requirements into the correct hierarchy required for an SRTM.

Requirement 1: The system shall provide confidentiality for data in transit and data at rest.

Requirement 2: The system shall use SSL, SSH, or SCP for all data transport.

Requirement 3: The system shall implement a file-level encryption scheme.

Requirement 4: The system shall provide integrity for all data at rest.

Requirement 5: The system shall perform CRC checks on all files.

- A. Level 1: Requirements 1 and 4; Level 2: Requirements 2, 3, and 5
- B. Level 1: Requirements 1 and 4; Level 2: Requirements 2 and 3 under 1, Requirement 5 under 4
- C. Level 1: Requirements 1 and 4; Level 2: Requirement 2 under 1, Requirement 5 under 4; Level 3: Requirement 3 under 2
- D. Level 1: Requirements 1, 2, and 3; Level 2: Requirements 4 and 5

Correct Answer: B

Confidentiality and integrity are two of the key facets of data security. Confidentiality ensures that sensitive information is not disclosed to unauthorized users; while integrity ensures that data is not altered by unauthorized users. These are Level 1 requirements.



Confidentiality is enforced through encryption of data at rest, encryption of data in transit, and access control. Encryption of data in transit is accomplished by using secure protocols such as PSec, SSL, PPTP, SSH, and SCP, etc.

Integrity can be enforced through hashing, digital signatures and CRC checks on the files.

In the SRTM hierarchy, the enforcement methods would fall under the Level requirement.

References:

Gregg, Michael, and Billy Haines, *CASP CompTIA Advanced Security Practitioner Study Guide*, John Wiley and Sons, Indianapolis, 2012, pp. 17-19, 20, 27-29

QUESTION 3

A small company's Chief Executive Officer (CEO) has asked its Chief Security Officer (CSO) to improve the company's security posture quickly with regard to targeted attacks. Which of the following should the CSO conduct FIRST?

- A. Survey threat feeds from services inside the same industry.
- B. Purchase multiple threat feeds to ensure diversity and implement blocks for malicious traffic.
- C. Conduct an internal audit against industry best practices to perform a qualitative analysis.
- D. Deploy a UTM solution that receives frequent updates from a trusted industry vendor.

Correct Answer: A

Security posture refers to the overall security plan from planning through to implementation and comprises technical and non-technical policies, procedures and controls to protect from both internal and external threats. From a security standpoint, one of the first questions that must be answered in improving the overall security posture of an organization is to identify where data resides. All the advances that were made by technology make this very difficult. The best way then to improve your company's security posture is to first survey threat feeds from services inside the same industry.

QUESTION 4

A mature organization with legacy information systems has incorporated numerous new processes and dependencies to manage security as its networks and infrastructure are modernized. The Chief Information Office has become increasingly frustrated with frequent releases, stating that the organization needs everything to work completely, and the vendor should already have those desires built into the software product. The vendor has been in constant communication with personnel and groups within the organization to understand its business process and capture new software requirements from users. Which of the following methods of software development is this organization's configuration management process using?

- A. Agile
- B. SDL
- C. Waterfall
- D. Joint application development

Correct Answer: A



In agile software development, teams of programmers and business experts work closely together, using an iterative approach.

QUESTION 5

Which of the following describes a risk and mitigation associated with cloud data storage?

- A. Risk: Shared hardware caused data leakage Mitigation: Strong encryption at rest
- B. Risk: Offsite replication Mitigation: Multi-site backups
- C. Risk: Data loss from de-duplication Mitigation: Dynamic host bus addressing
- D. Risk: Combined data archiving Mitigation: Two-factor administrator authentication

Correct Answer: A

With cloud data storage, the storage provider will have large enterprise SANs providing large pools of storage capacity. Portions of the storage pools are assigned to customers. The risk is that multiple customers are storing their data on the same physical hardware storage devices. This presents a risk (usually a very small risk, but a risk all the same) of other customers using the same cloud storage hardware being able to view your data. The mitigation of the risk is to encrypt your data stored on the SAN. Then the data would be unreadable even if another customer was able to access it.

[RC0-C02 PDF Dumps](#)

[RC0-C02 VCE Dumps](#)

[RC0-C02 Study Guide](#)