SY0-701 Q&As

CompTIA Security+ 2024

Pass CompTIA SY0-701 Exam with 100% Guarantee

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

https://www.pass4itsure.com/sy0-701.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

Which of the following security concepts is the best reason for permissions on a human resources fileshare to follow the principle of least privilege?

A. Integrity

B. Availability

C. Confidentiality

D. Non-repudiation

Correct Answer: C

Confidentiality is the security concept that ensures data is protected from unauthorized access or disclosure. The principle of least privilege is a technique that grants users or systems the minimum level of access or permissions that they need to perform their tasks, and nothing more. By applying the principle of least privilege to a human resources fileshare, the permissions can be restricted to only those who have a legitimate need to access the sensitive data, such as HR staff, managers, or auditors. This can prevent unauthorized users, such as hackers, employees, or contractors, from accessing, copying, modifying, or deleting the data. Therefore, the principle of least privilege can enhance the confidentiality of the data on the fileshare. Integrity, availability, and non- repudiation are other security concepts, but they are not the best reason for permissions on a human resources fileshare to follow the principle of least privilege. Integrity is the security concept that ensures data is accurate and consistent, and protected from unauthorized modification or corruption. Availability is the security concept that ensures data is accessible and usable by authorized users or systems when needed. Non-repudiation is the security concept that ensures the authenticity and accountability of data and actions, and prevents the denial of involvement or responsibility. While these concepts are also important for data security, they are not directly related to the level of access or permissions granted to users or systems.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17, 372-373

QUESTION 2

An organization disabled unneeded services and placed a firewall in front of a business- critical legacy system. Which of the following best describes the actions taken by the organization?

A. Exception

B. Segmentation

C. Risk transfer

D. Compensating controls

Correct Answer: D

Compensating controls are alternative security measures that are implemented when the primary controls are not feasible, cost-effective, or sufficient to mitigate the risk. In this case, the organization used compensating controls to protect the

legacy system from potential attacks by disabling unneeded services and placing a firewall in front of it. This reduced the attack surface and the likelihood of exploitation.

References:

Official CompTIA Security+ Study Guide (SY0-701), page 29 Security Controls - CompTIA Security+ SY0-701 - 1.1 1

QUESTION 3

Which of the following describes the maximum allowance of accepted risk?

A. Risk indicator

B. Risk level

C. Risk score

D. Risk threshold

Correct Answer: D

Risk threshold is the maximum amount of risk that an organization is willing to accept for a given activity or decision. It is also known as risk appetite or risk tolerance. Risk threshold helps an organization to prioritize and allocate resources for risk management. Risk indicator, risk level, and risk score are different ways of measuring or expressing the likelihood and impact of a risk, but they do not describe the maximum allowance of accepted risk. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 34; Accepting Risk: Definition, How It Works, and Alternatives

QUESTION 4

Which of the following is used to add extra complexity before using a one-way data transformation algorithm?

A. Key stretching

B. Data masking

C. Steganography

D. Salting

Correct Answer: D

Salting is the process of adding extra random data to a password or other data before applying a one-way data transformation algorithm, such as a hash function. Salting increases the complexity and randomness of the input data, making it

harder for attackers to guess or crack the original data using precomputed tables or brute force methods. Salting also helps prevent identical passwords from producing identical hash values, which could reveal the passwords to attackers who

have access to the hashed data. Salting is commonly used to protect passwords stored in databases or transmitted over networks.

References:

Passwords technical overview

Encryption, hashing, salting ?what\\'s the difference? Salt (cryptography)

QUESTION 5

A bank insists all of its vendors must prevent data loss on stolen laptops. Which of the following strategies is the bank requiring?

A. Encryption at rest

B. Masking

C. Data classification

D. Permission restrictions

Correct Answer: A

Encryption at rest is a strategy that protects data stored on a device, such as a laptop, by converting it into an unreadable format that can only be accessed with a decryption key or password. Encryption at rest can prevent data loss on stolen laptops by preventing unauthorized access to the data, even if the device is physically compromised. Encryption at rest can also help comply with data privacy regulations and standards that require data protection. Masking, data classification, and permission restrictions are other strategies that can help protect data, but they may not be sufficient or applicable for data stored on laptops. Masking is a technique that obscures sensitive data elements, such as credit card numbers, with random characters or symbols, but it is usually used for data in transit or in use, not at rest. Data classification is a process that assigns labels to data based on its sensitivity and business impact, but it does not protect the data itself. Permission restrictions are rules that define who can access, modify, or delete data, but they may not prevent unauthorized access if the laptop is stolen and the security controls are bypassed.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 17-18, 372-373