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.geekcert.com/sy0-701.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

The Chief Information Security Officer wants to prevent exfiltration of sensitive information from employee cell phones when using public USB power charging stations. Which of the following would be the BEST solution to Implement?

A. DLP

B. USB data blocker

C. USB OTG

D. Disabling USB ports

Correct Answer: B

The best solution to prevent exfiltration of sensitive information from employee cell phones when using public USB power charging stations would be to use a USB data blocker. A USB data blocker is a device that can be used to physically block the data pins on a USB cable, preventing data transfer while still allowing the device to be charged. This would prevent employees from accidentally or maliciously transferring sensitive data from their cell phones to the public charging station. Options A, C, and D would not be effective in preventing this type of data exfiltration

QUESTION 2

An engineer moved to another team and is unable to access the new team\\'s shared folders while still being able to access the shared folders from the former team. After opening a ticket, the engineer discovers that the account was never moved to the new group. Which of the following access controls is most likely causing the lack of access?

A. Role-based

B. Discretionary

C. Time of day

D. Least privilege

Correct Answer: A

QUESTION 3

Which of the following would be most useful in determining whether the long-term cost to transfer a risk is less than the impact of the risk?

A. ARO

B. RTO

C. RPO

D. ALE

E. SLE

Correct Answer: D

QUESTION 4

While troubleshooting a firewall configuration, a technician determines that a "deny any" policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable.

Which of the following actions would prevent this issue?

A. Documenting the new policy in a change request and submitting the request to change management

B. Testing the policy in a non-production environment before enabling the policy in the production network

C. Disabling any intrusion prevention signatures on the \\'deny any* policy prior to enabling the new policy

D. Including an \\'allow any1 policy above the \\'deny any* policy

Correct Answer: B

A firewall policy is a set of rules that defines what traffic is allowed or denied on a network. A firewall policy should be carefully designed and tested before being implemented, as a misconfigured policy can cause network disruptions or security breaches. A common best practice is to test the policy in a non-production environment, such as a lab or a simulation, before enabling the policy in the production network. This way, the technician can verify the functionality and performance of the policy, and identify and resolve any issues or conflicts, without affecting the live network. Testing the policy in a non-production environment would prevent the issue of the `deny any\\' policy causing several company servers to become unreachable, as the technician would be able to detect and correct the problem before applying the policy to the production network. Documenting the new policy in a change request and submitting the request to change management is a good practice, but it would not prevent the issue by itself. Change management is a process that ensures that any changes to the network are authorized, documented, and communicated, but it does not guarantee that the changes are error-free or functional. The technician still needs to test the policy before implementing it. Disabling any intrusion prevention signatures on the `deny any\\' policy prior to enabling the new policy would not prevent the issue, and it could reduce the security of the network. Intrusion prevention signatures are patterns that identify malicious or unwanted traffic, and allow the firewall to block or alert on such traffic. Disabling these signatures would make the firewall less effective in detecting and preventing attacks, and it would not affect the reachability of the company servers. Including an `allow any\\' policy above the `deny any\\' policy would not prevent the issue, and it would render the `deny any\\' policy useless. A firewall policy is processed from top to bottom, and the first matching rule is applied. An `allow any\\' policy would match any traffic and allow it to pass through the firewall, regardless of the source, destination, or protocol. This would negate the purpose of the `deny any\\' policy, which is to block any traffic that does not match any of the previous rules. Moreover, an `allow any\\' policy would create a security risk, as it would allow any unauthorized or malicious traffic to enter or exit the network.

References: CompTIA Security+ SY0-701 Certification Study Guide, page 204- 205; Professor Messer\\'s CompTIA SY0-701 Security+ Training Course, video 2.1 - Network Security Devices, 8:00 - 10:00.

QUESTION 5

The application development teams have been asked to answer the following questions:

1.

Does this application receive patches from an external source?

2.

Does this application contain open-source code?

3.

Is this application accessible by external users?

4.

Does this application meet the corporate password standard?

Which of the following are these questions part of?

A. Risk control self-assessment

B. Risk management strategy

C. Risk acceptance

D. Risk matrix

Correct Answer: A

The questions listed are part of a Risk Control Self-Assessment (RCSA), which is a process where teams evaluate the risks associated with their operations and assess the effectiveness of existing controls. The questions focus on aspects

such as patch management, the use of open-source code, external access, and compliance with corporate standards, all of which are critical for identifying and mitigating risks.

References:

CompTIA Security+ SY0-701 Course Content: The course discusses various risk management processes, including self-assessments that help in identifying and managing risks within the organization.