SY0-701$^{\text{Q\&As}}$

CompTIA Security+ 2024

Pass CompTIA SY0-701 Exam with 100% Guarantee

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

https://www.pass2lead.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

A company has begun labeling all laptops with asset inventory stickers and associating them with employee IDs. Which of the following security benefits do these actions provide? (Choose two.)

A. If a security incident occurs on the device, the correct employee can be notified.

B. The security team will be able to send user awareness training to the appropriate device.

C. Users can be mapped to their devices when configuring software MFA tokens.

D. User-based firewall policies can be correctly targeted to the appropriate laptops.

E. When conducting penetration testing, the security team will be able to target the desired laptops.

F. Company data can be accounted for when the employee leaves the organization.

Correct Answer: AF

Labeling all laptops with asset inventory stickers and associating them with employee IDs can provide several security benefits for a company. Two of these benefits are:

A. If a security incident occurs on the device, the correct employee can be notified. An asset inventory sticker is a label that contains a unique identifier for a laptop, such as a serial number, a barcode, or a QR code. By associating this identifier with an employee ID, the security team can easily track and locate the owner of the laptop in case of a security incident, such as a malware infection, a data breach, or a theft. This way, the security team can notify the correct employee about the incident, and provide them with the necessary instructions or actions to take, such as changing passwords, scanning for viruses, or reporting the loss. This can help to contain the incident, minimize the damage, and prevent further escalation.

F. Company data can be accounted for when the employee leaves the organization. When an employee leaves the organization, the company needs to ensure that all the company data and assets are returned or deleted from the employee\\'s laptop. By labeling the laptop with an asset inventory sticker and associating it with an employee ID, the company can easily identify and verify the laptop that belongs to the departing employee, and perform the appropriate data backup, wipe, or transfer procedures. This can help to protect the company data from unauthorized access, disclosure, or misuse by the former employee or any other party. The other options are not correct because they are not related to the security benefits of labeling laptops with asset inventory stickers and associating them with employee IDs. B. The security team will be able to send user awareness training to the appropriate device. User awareness training is a type of security education that aims to improve the knowledge and behavior of users regarding security threats and best practices. The security team can send user awareness training to the appropriate device by using the email address, username, or IP address of the device, not the asset inventory sticker or the employee ID. C. Users can be mapped to their devices when configuring software MFA tokens. Software MFA tokens are a type of multi-factor authentication that uses a software application to generate a one-time password or a push notification for verifying the identity of a user. Users can be mapped to their devices when configuring software MFA tokens by using the device ID, phone number, or email address of the device, not the asset inventory sticker or the employee ID. D. User-based firewall policies can be correctly targeted to the appropriate laptops. User-based firewall policies are a type of firewall rules that apply to specific users or groups of users, regardless of the device or location they use to access the network. User-based firewall policies can be correctly targeted to the appropriate laptops by using the username, domain, or certificate of the user, not the asset inventory sticker or the employee ID. E. When conducting penetration testing, the security team will be able to target the desired laptops. Penetration testing is a type of security assessment that simulates a real-world attack on a network or system to identify and exploit vulnerabilities. When conducting penetration testing, the security team will be able to target the desired laptops by using the IP address, hostname, or MAC address of the laptop, not the asset inventory sticker or the employee ID.

References: CompTIA Security+ Study Guide (SY0-701), Chapter 1: General Security Concepts, page 17. Professor

Messer\\'s CompTIA SY0-701 Security+ Training Course, Section 1.4: Asset Management, video: Asset Inventory (6:12).

QUESTION 2

A company is developing a critical system for the government and storing project information on a fileshare. Which of the following describes how this data will most likely be classified? (Select two).

A. Private

B. Confidential

C. Public

D. Operational

E. Urgent

F. Restricted

Correct Answer: BF

Data classification is the process of assigning labels to data based on its sensitivity and business impact. Different organizations and sectors may have different data classification schemes, but a common one is the following1:

Public: Data that can be freely disclosed to anyone without any harm or risk. Private: Data that is intended for internal use only and may cause some harm or risk if disclosed.

Confidential: Data that is intended for authorized use only and may cause significant harm or risk if disclosed.

Restricted: Data that is intended for very limited use only and may cause severe harm or risk if disclosed.

In this scenario, the company is developing a critical system for the government and storing project information on a fileshare. This data is likely to be classified as confidential and restricted, because it is not meant for public or private use,

and it may cause serious damage to national security or public safety if disclosed. The government may also have specific requirements or regulations for handling such data, such as encryption, access control, and auditing2.

References: 1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17 2: Data Classification Practices: Final Project Description Released

QUESTION 3

Which of the following is the MOST effective control against zero-day vulnerabilities?

A. Network segmentation

B. Patch management

C. Intrusion prevention system

D. Multiple vulnerability scanners

Correct Answer: A

IPS can only protect against known host and application-based attacks and exploits. IPS inspects traffic against signatures and anomalies, it does cover a broad spectrum of attack types, most of them signature-based, and signatures alone cannot protect against zero-day attacks. (www.rawcode7.medium.com)

However, with network segmentation, you\\'re able to isolate critical assets into different segments. And when a zero-day attack occurs, you\\'re not at risk of losing all and are able to isolate the attack\\'s effect to one segment.

QUESTION 4

A systems administrator wants to prevent users from being able to access data based on their responsibilities. The administrator also wants to apply the required access structure via a simplified format. Which of the following should the administrator apply to the site recovery resource group?

A. RBAC

B. ACL

C. SAML

D. GPO

Correct Answer: A

RBAC stands for Role-Based Access Control, which is a method of restricting access to data and resources based on the roles or responsibilities of users. RBAC simplifies the management of permissions by assigning roles to users and granting access rights to roles, rather than to individual users. RBAC can help enforce the principle of least privilege and reduce the risk of unauthorized access or data leakage. The other options are not as suitable for the scenario as RBAC, as they either do not prevent access based on responsibilities, or do not apply a simplified format.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 133 1

QUESTION 5

Which of the following are cases in which an engineer should recommend the decommissioning of a network device? (Select two).

A. The device has been moved from a production environment to a test environment.

B. The device is configured to use cleartext passwords.

C. The device is moved to an isolated segment on the enterprise network.

D. The device is moved to a different location in the enterprise.

E. The device\\'s encryption level cannot meet organizational standards.

F. The device is unable to receive authorized updates.

Correct Answer: E

An engineer should recommend the decommissioning of a network device when the device poses a security risk or a compliance violation to the enterprise environment. A device that cannot meet the encryption standards or receive authorized updates is vulnerable to attacks and breaches, and may expose sensitive data or compromise network integrity. Therefore, such a device should be removed from the network and replaced with a more secure and updated one.

References CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, Section 2.2, page 671 CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 2, Question 16, page 512