SY0-601 Q&As

CompTIA Security+

Pass CompTIA SY0-601 Exam with 100% Guarantee

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

https://www.pass4itsure.com/sy0-601.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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

QUESTION 2

The most recent vulnerability scan flagged the domain controller with a critical vulnerability. The systems administrator researched the vulnerability and discovered the domain controller does not run the associated application with the vulnerability. Which of the following steps should the administrator take next?

A. Ensure the scan engine is configured correctly.

B. Apply a patch to the domain controller.

C. Research the CVE.

D. Document this as a false positive.

Correct Answer: D

QUESTION 3

A security analyst has identified malware spreading through the corporate network and has activated the CSIRT

Which of the following should the analyst do NEXT?

A. Review how the malware was introduced to the network

B. Attempt to quarantine all infected hosts to limit further spread

C. Create help desk tickets to get infected systems reimaged

D. Update all endpoint antivirus solutions with the latest updates

Correct Answer: B

Phases in the Incident Response Plan

1.

Preparation: The organization plans out how they will respond to attack, this can involve:

2.

Identification: Detecting and determining whether an incident has occurred.

3.

Containment: Once a threat has been identified, the organization must limit or prevent any further damage. 4. Eradication: The removal of the threat

5.

Recovery: Restoring systems affected by the incident

6.

Lessons Learned: Where the organization reviews their incident response and prepare for a future attack

QUESTION 4

A police department is using the cloud to share information city officials.

Which of the cloud models describes this scenario?

A. Hybrid

B. private

C. pubic

D. Community

Correct Answer: D

A community cloud model describes a scenario where a cloud service is shared among multiple organizations that have common goals, interests, or requirements. A community cloud can be hosted by one of the organizations, a third-party provider, or a combination of both. A community cloud can offer benefits such as cost savings, security, compliance, and collaboration. A police department using the cloud to share information with city officials is an example of a community cloud model.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.ibm.com/cloud/learn/community-cloud

QUESTION 5

Two organizations plan to collaborate on the evaluation of new SIEM solutions for their respective companies. A combined effort from both organizations\\' SOC teams would speed up the effort. Which of the following can be written to document this agreement?

A. MOU

B. ISA

C. SLA

D. NDA

Correct Answer: A

A document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal MOA/MOU that defines high- level roles and responsibilities in management of a cross-domain connection.

https://csrc.nist.gov/glossary/term/interconnection_security_agreement