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.geekcert.com/sy0-601.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 would be indicative of a hidden audio file found inside of a piece of source code?

A. Steganography

B. Homomotphic encryption

C. Cipher surte

D. Blockchain

Correct Answer: A

Steganography is the technique of hiding secret data within an ordinary, non- secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data. The word steganography is derived from the Greek words steganos (meaning hidden or covered) and the Greek root graph (meaning to write).

QUESTION 2

Which of the following agreements defines response time, escalation points, and performance metrics?

A. BPA

B. MOA

C. NDA

D. SLA

Correct Answer: D

An SLA (Service Level Agreement) is a formal agreement between a service provider and a customer that defines the terms and conditions of the service being provided. It outlines the agreed-upon response time, escalation points, performance metrics, and other service-related parameters. SLAs are commonly used in various business relationships to establish clear expectations and ensure that the service provider meets the agreed-upon standards of service delivery.

QUESTION 3

Phishing and spear-phishing attacks have been occurring more frequently against a company\\'s staff. Which of the following would MOST likely help mitigate this issue?

A. DNSSEC and DMARC

B. DNS query logging

C. Exact mail exchanger records in the DNS

D. The addition of DNS conditional forwarders

Correct Answer: C

QUESTION 4

Which of the following is the MOST effective way to detect security flaws present on third- party libraries embedded on software before it is released into production?

A. Employ different techniques for server- and client-side validations.

B. Use a different version control system for third-party libraries.

C. Implement a vulnerability scan to assess dependencies earlier on SDLC.

D. Increase the number of penetration tests before software release.

Correct Answer: C

The most effective way to detect security flaws present on third-party libraries embedded on software before it is released into production is to implement a vulnerability scan to assess dependencies earlier on the SDLC, or software development life cycle. A vulnerability scan is a type of security assessment that involves identifying and analyzing potential vulnerabilities in a system or application. By conducting a vulnerability scan earlier on in the SDLC, the development team can identify any security flaws in the third-party libraries before the software is released into production. This can help prevent security issues from being introduced into the production environment and ensure that the software is secure and compliant. Employing different techniques for server- and client-side validations, using a different version control system for third-party libraries, and increasing the number of penetration tests are not directly related to detecting security flaws in third-party libraries.

QUESTION 5

The marketing department at a retail company wants to publish an internal website to the internet so it is reachable by a limited number of specific, external service providers in a secure manner. Which of the following configurations would be BEST to fulfil this requirement?

A. NAC

B. ACL

C. WAF

D. NAT

Correct Answer: B