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.pass2lead.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 can be used to detect a hacker who is stealing company data over port 80?

A. Web application scan

B. Threat intelligence

C. Log aggregation

D. Packet capture

Correct Answer: D

Using a SIEM tool to monitor network traffic in real-time and detect any anomalies or malicious activities Monitoring all network protocols and ports to detect suspicious volumes of traffic or connections to uncommon IP addresses Monitoring for outbound traffic patterns that indicate malware communication with command and control servers, such as beaconing or DNS tunneling Using a CASB tool to control access to cloud resources and prevent data leaks or downloads Encrypting data at rest and in transit and enforcing strong authentication and authorization policies

---

QUESTION 2

Which of the following documents provides guidance regarding the recommended deployment of network security systems from the manufacturer?

A. Cloud control matrix

B. Reference architecture

C. NIST RMF

D. CIS Top 20

Correct Answer: B

A reference architecture is a document or set of documents that provides recommended structures and integrations of IT products and services to form a solution.

QUESTION 3

A company\\'s Chief Information Security Officer (CISO) recently warned the security manager that the company\\'s Chief Executive Officer (CEO) is planning to publish a controversial option article in a national newspaper, which may result in new cyberattacks Which of the following would be BEST for the security manager to use in a threat mode?

A. Hacktivists

B. White-hat hackers

C. Script kiddies

D. Insider threats

Correct Answer: A

First the executive is in a pretty high position to be a threat at all. Because an insider threat for me is someone with intention to harm the company. Second, by uploading an controversial article isn\\'t going to harm the company directly.

QUESTION 4

A recent security assessment revealed that an actor exploited a vulnerable workstation within an organization and has persisted on the network for several months. The organization realizes the need to reassess its security strategy for mitigating risks within the perimeter. Which of the following solutions would BEST support the organization\\'s strategy?

A. FIM

B. DLP

C. EDR

D. UTM

Correct Answer: C

FIM File Integrity Monitoring DLP Data Loss Prevention EDR Endpoint Detection and Response UTM Unified Threat Management

I think the answer is EDR (when signature detection is not enough -> behavioral analysis, machine learning) update from UTM is NGFF

QUESTION 5

Which of the following should a technician consider when selecting an encryption method for data that needs to remain confidential for a specific length of time?

A. The key length of the encryption algorithm

B. The encryption algorithm\\'s longevity

C. A method of introducing entropy into key calculations

D. The computational overhead of calculating the encryption key

Correct Answer: B

SY0-601 Student guide, "In another sense, longevity is the consideration of how long data must be kept secure. If you assume that a ciphertext will be exposed at some point, how long must that ciphertext resist cryptanalysis? For example, imagine an NSA operative\\'s laptop is stolen. The thief cannot hope to break the encryption with current computing resources, but how long must that encryption mechanism continue to protect the data? If advances in cryptanalysis will put it at risk within 5 years, or 10 years, or 20 years, could a more secure algorithm have been chosen?"