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

QUESTION 1

A security administrator currently spends a large amount of time on common security tasks, such as report generation, phishing investigations, and user provisioning and deprovisioning. This prevents the administrator from spending time on other security projects. The business does not have the budget to add more staff members. Which of the following should the administrator attempt?

A. DAC

B. ABAC

C. SCAP

D. SOAR

Correct Answer: D

Reference: https://searchsecurity.techtarget.com/definition/SOAR

QUESTION 2

A company wants to deploy decoy systems alongside production systems in order to entice threat actors and to learn more about attackers. Which of the following BEST describes these systems?

A. DNS sinkholes

B. Hafieypots

C. Virtual machines

D. Neural networks

Correct Answer: B

Honeypots are decoy systems or resources intentionally set up by an organization to attract and monitor unauthorized users, attackers, or malware. These systems are isolated from the production network and have no legitimate purpose, making any activity on them highly suspicious. The primary goal of honeypots is to gather information about the tactics, techniques, and procedures used by attackers and to learn more about their motives and potential threats to the organization.

QUESTION 3

An organization would like to remediate the risk associated with its cloud service provider not meeting its advertised 99.999% availability metrics. Which of the following should the organization consult for the exact requirements for the cloud provider?

A. SLA

B. BPA

C. NDA

D. MOU

Correct Answer: A

QUESTION 4

An employee used a corporate mobile device during a vacation Multiple contacts were modified in the device vacation.

Which of the following method did attacker to insert the contacts without having \\'Physical access to device?

A. Jamming

B. BluJacking

C. Disassoaatm

D. Evil twin

Correct Answer: B

bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers. Bluejacking does not involve device hijacking, despite what the name implies. In this context, a human might say that the best answer to the question is B. BluJacking, because it is a method that can insert contacts without having physical access to the device.

QUESTION 5

An organization recently released a zero-trust policy that will enforce who is able to remotely access certain data. Authenticated users who access the data must have a need to know, depending on their level of permissions.

Which of the following is the first step the organization should take when implementing the policy?

A. Determine a quality CASB solution.

B. Configure the DLP policies by user groups.

C. Implement agentless NAC on boundary devices.

D. Classify all data on the file servers.

Correct Answer: D

zero trust is a security strategy that assumes breach and verifies each request as though it originates from an untrusted network12. A zero trust policy is a set of "allow rules" that specify conditions for accessing certain resources3. According to one source4, the first step in implementing a zero trust policy is to identify and classify all data and assets in the organization. This helps to determine the level of sensitivity and risk associated with each resource and apply appropriate access controls. Classifying all data on the file servers is the first step in implementing a zero trust policy because it helps to determine the level of sensitivity and risk associated with each resource and apply appropriate access controls. Reference: Zero Trust implementation guidance | Microsoft Learn