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.passapply.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

The Chief Information Security Officer directed a risk reduction in shadow IT and created a policy requiring all unsanctioned high-risk SaaS applications to be blocked from user access.

Which of the following is the BEST security solution to reduce this risk?

A. CASB

B. VPN concentrator

C. MFA

D. VPC endpoint

Correct Answer: A

The best security solution to reduce the risk of shadow IT and unsanctioned high-risk SaaS applications is a Cloud Access Security Broker (CASB). A CASB is a security solution that is designed to provide visibility and control over cloud applications and services. It can be used to block access to unsanctioned applications and to enforce security policies and compliance requirements for cloud services. In this case, the CASB would be used to block access to unsanctioned high-risk SaaS applications, reducing the risk of shadow IT and helping the organization to maintain control over its cloud environment. Options B, C, and D are not specifically related to reducing the risk of shadow IT and unsanctioned SaaS applications. A VPN concentrator is a network device that is used to manage and terminate VPN connections, MFA is a security control that requires multiple factors for authentication, and a VPC endpoint is a networking feature that allows private access to AWS services.

QUESTION 2

Which of the following would be the BEST resource for a software developer who is looking to improve secure coding practices for web applications?

A. OWASP

B. Vulnerability scan results

C. NIST CSF

D. Third-party libraries

Correct Answer: A

QUESTION 3

A security analyst is evaluating the risks of authorizing multiple security solutions to collect data from the company\\'s cloud environment Which of the following is an immediate consequence of these integrations?

A. Non-compliance with data sovereignty rules

B. Loss of the vendor\\'s interoperability support

C. Mandatory deployment of a SIEM solution

D. Increase in the attack surface

Correct Answer: D

While Non-compliance with data sovereignty rules is an implication of having multiple cloud providers at DIFFERENT countries, this is not specified in the question, besides, they are security solutions, which typically means they will not collect any kind of PII, PHI, SPI

QUESTION 4

A security administrator checks the table of a network switch, which shows the following output:

VLAN	Physical address	Type	Port
1	001a:42ff:5113	Dynamic	GE0/5
1	0faa:abcf:ddee	Dynamic	GE0/5
1	c6a9:6b16:758e	Dynamic	GE0/5
1	a3aa:b6a3:1212	Dynamic	GE0/5
1	8025:2ad8:bfac	Dynamic	GE0/5
1	b839:f995:a00a	Dynamic	GE0/5

Which of the following is happening to this switch?

A. MAC Flooding

B. DNS poisoning

C. MAC cloning

D. ARP poisoning

Correct Answer: A

The MAC Flooding is an attacking method intended to compromise the security of the network switches. Usually, the switches maintain a table structure called MAC Table. This MAC Table consists of individual MAC addresses of the host computers on the network which are connected to ports of the switch. This table allows the switches to direct the data out of the ports where the recipient is located.

The aim of the MAC Flooding is to takedown this MAC Table. In a typical MAC Flooding attack, the attacker sends Ethernet Frames in a huge number. When sending many Ethernet Frames to the switch, these frames will have various sender addresses. The intention of the attacker is consuming the memory of the switch that is used to store the MAC address table. The MAC addresses of legitimate users will be pushed out of the MAC Table. Now the switch cannot deliver the incoming data to the destination system. So considerable number of incoming frames will be flooded at all ports.

https://www.interserver.net/tips/kb/mac-flooding-prevent/

QUESTION 5

A smart switch has the ability to monitor electrical levels and shut off power to a building in the event of power surge or other fault situation. The switch was installed on a wired network in a hospital and is monitored by the facilities department via a cloud application.

The security administrator isolated the switch on a separate VLAN and set up a patch routine. Which of the following steps should also be taken to harden the smart switch?

A. Set up an air gap for the switch.

B. Change the default password for the switch.

C. Place the switch In a Faraday cage.

D. Install a cable lock on the switch

Correct Answer: B

A. Set up an air gap for the switch. - it uses cloud monitoring, this doesn\\'t work

B. Change the default password for the switch. - only one that makes sense, seems to easy, but the other answers are ridiculous given the information.

C. Place the switch in a Faraday cage. - this is a red haring

D. Install a cable lock on the switch. - you don\\'t do this with switches, like physically locking a switch in place - you could put cable locks on the individual patch cable, but not the switch itself, this is typically secured behind a locked door or locked rack door.