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 security operations analyst is using the company\\'s SIEM solution to correlate alerts. Which of the following stages of the incident response process is this an example of?

A. Eradication

B. Recovery

C. Identification

D. Preparation

Correct Answer: C

C: Identification

Incident response lifecycle:

-preparation

-detection and analysis

-containment, eradication, recovery

-post-incident activity

QUESTION 2

A desktop support technician recently installed a new document-scanning software program on a computer. However, when the end user tried to launch the program, it did not respond. Which of the following is MOST likely the cause?

A. A new firewal rule is needed to access the application.

B. The system was quarantined for missing software updates.

C. The software was not added to the application whitelist.

D. The system was isolated from the network due to infected software

Correct Answer: C

Firewall is irrelevant to the question. Firewall rules determine if traffic will go trough or get blocked. The firewall has no access or control over processes or applications on the system. The issue is that the application is not whitelisted, which prevents it from booting.

QUESTION 3

Which of the following would an organization use to assign a value to risks based on probability of occurrence and impact?

A. Risk matrix

B. Risk register

C. Risk appetite

D. Risk mitigation plan

Correct Answer: B

QUESTION 4

An amusement park is implementing a btomelnc system that validates customers\\' fingerpnnts to ensure they are not sharing tickets The park\\'s owner values customers above all and would prefer customers\\' convenience over security For this reason which of the following features should the security team prioritize FIRST?

A. Low FAR

B. Low efficacy

C. Low FRR

D. Low CER

Correct Answer: C

FAR (False Acceptance Rate)

FRR (False Rejection Rate)

CER (Crossover Error Rate) AKA ERR (Equal Error Rate)

since he is willing to sacrifice Security for Customer Service, Best way to understand this is.

FAR has to go up in order for FRR to go down.

typical business practice is in the middle of both which would be near the CER.

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.