CS0-003 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/cs0-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

Which of the following ICS network protocols has no inherent security functions on TCP port 502?

A. CIP

B. DHCP

C. SSH

D. Modbus

Correct Answer: D

Modbus is an industrial control system (ICS) network protocol that is used for communication between devices such as sensors, controllers, actuators, and monitors. Modbus has no inherent security functions on TCP port 502, which is the default port for Modbus TCP/IP communication. Modbus does not provide any encryption, authentication, or integrity protection for the data transmitted over the network, making it vulnerable to various attacks such as replay, modification, spoofing, or denial-of-service.

QUESTION 2

An analyst receives threat intelligence regarding potential attacks from an actor with seemingly unlimited time and resources. Which of the following best describes the threat actor attributed to the malicious activity?

A. Insider threat

B. Ransomware group

C. Nation-state

D. Organized crime

Correct Answer: C

QUESTION 3

An organization has the following risk mitigation policies

Risks without compensating controls will be mitigated first it the nsk value is greater than $50,000 Other nsk mitigation will be pnontized based on risk value.

The following risks have been identified: Which of the following is the ordei of priority for risk mitigation from highest to lowest?

Risk	Probability	Impact	Compensating control?
A	80%	$100,000	Y
B	20%	$500,000	Y
C	50%	$120,000	N
D	40%	$80,000	N

A. A, C, D, B

B. B, C, D, A

C. C, B, A, D

D. C. D, A, B

E. D, C, B, A

Correct Answer: C

The order of priority for risk mitigation from highest to lowest is C, B, A, D. This order is based on applying the risk mitigation policies of the organization. According to the first policy, risks without compensating controls will be mitigated first if the risk value is greater than $50,000. Risk C has no compensating controls and a risk value of $75,000, so it is the highest priority. Risk B also has no compensating controls, but a risk value of $40,000, so it is the second priority. According to the second policy, other risk mitigation will be prioritized based on risk value. Risk A has a risk value of $60,000 and a compensating control of encryption, so it is the third priority. Risk D has a risk value of $50,000 and a compensating control of backup power supply, so it is the lowest priority.

QUESTION 4

A malicious actor has gained access to an internal network by means of social engineering. The actor does not want to lose access in order to continue the attack. Which of the following best describes the current stage of the Cyber Kill Chain that the threat actor is currently operating in?

A. Weaponization

B. Reconnaissance

C. Delivery

D. Exploitation

Correct Answer: D

The Cyber Kill Chain is a framework that describes the stages of a cyberattack from reconnaissance to actions on objectives. The exploitation stage is where attackers take advantage of the vulnerabilities they have discovered in previous stages to further infiltrate a" objectives. In this case, the malicious actor has gained access to an internal network by means of social engineering and does not want to lose access in order to continue the attack. This indicates that the actor is in the exploitation stage of the Cyber Kill Chain. Official Reference: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

QUESTION 5

After identifying a threat, a company has decided to implement a patch management program to remediate vulnerabilities. Which of the following risk management principles is the company exercising?

A. Transfer

B. Accept

C. Mitigate

D. Avoid

Correct Answer: C

Mitigate is the best term to describe the risk management principle that the company is exercising, as it means to reduce the likelihood or impact of a risk. By implementing a patch management program to remediate vulnerabilities, the company is mitigating the threat of cyberattacks that could exploit those vulnerabilities and compromise the security or functionality of the systems. The other terms are not as accurate as mitigate, as they describe different risk management principles. Transfer means to shift the responsibility or burden of a risk to another party, such as an insurer or a contractor. Accept means to acknowledge the existence of a risk and decide not to take any action to reduce it, usually because the risk is low or the cost of mitigation is too high. Avoid means to eliminate the possibility of a risk by changing the plans or activities that could cause it, such as cancelling a project or discontinuing a service

Reference: https://safetyculture.com/topics/risk-management/