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.pass2lead.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

The Chief Executive Officer of an organization recently heard that exploitation of new attacks in the industry was happening approximately 45 days after a patch was released. Which of the following would best protect this organization?

A. A mean time to remediate of 30 days

B. A mean time to detect of 45 days

C. A mean time to respond of 15 days

D. Third-party application testing

Correct Answer: A

A mean time to remediate (MTTR) is a metric that measures how long it takes to fix a vulnerability after it is discovered. A MTTR of 30 days would best protect the organization from the new attacks that are exploited 45 days after a patch is released, as it would ensure that the vulnerabilities are fixed before they are exploited

---

QUESTION 2

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 3

A recent penetration test discovered that several employees were enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. Which of the following would best address this issue?

A. Increasing training and awareness for all staff

B. Ensuring that malicious websites cannot be visited

C. Blocking all scripts downloaded from the internet

D. Disabling all staff members' ability to run downloaded applications

Correct Answer: A

QUESTION 4

Which of the following best describes the process of requiring remediation of a known threat within a given time frame?

A. SLA

B. MOU

C. Best-effort patching

D. Organizational governance

Correct Answer: A

An SLA is a formal agreement between two parties that defines the level of service, responsibilities, and expectations. It often includes specific terms related to the time frame within which certain actions or services must be performed. Requiring remediation of a known threat within a given time frame can be part of an SLA related to cybersecurity or incident response, ensuring that security issues are addressed promptly and effectively.

QUESTION 5

A technician is analyzing output from a popular network mapping tool for a PCI audit: Which of the following best describes the output?

```
PORT STATE SERVICE VERSION
22/tcp open ssh Cisco SSH 1.25 (protocol 2.0)
443/tcp open ssl/http OpenResty web app server
|_http-server-header: openresty
| ssl-enum-ciphers:
| TLSv1.1:
| ciphers:
| TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
| compressors:
| NULL
| cipher preference: server
| warnings:
| Insecure certificate signature (SHA1), score capped at F
| TLSv1.2:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - F
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - F
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - F
| TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - F
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - F
| TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - F
| TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - F
| TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - F
| TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
| compressors:
| NULL
| cipher preference: server
| warnings:
| Insecure certificate signature (SHA1), score capped at F
|_ least strength: F
MAC Address: MAC ADDRESS(Cisco Systems)
Service Info: OS: IOS; CPE: cpe:/o:cisco:ios
Service detection performed. Please report any incorrect results at <REDACTED>.
<REDACTED> done: 1 IP address (1 host up) scanned in 16.47 seconds
```

A. The host is not up or responding.

B. The host is running excessive cipher suites.

C. The host is allowing insecure cipher suites.

D. The Secure Shell port on this host is closed.

Correct Answer: C