CS0-003$^{\text{Q\&As}}$

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

QUESTION 1

A security analyst recently implemented a new vulnerability scanning platform. The initial scan of 438 hosts found the following vulnerabilities:

210 critical 1,854 high 1,786 medium 48 low

The analyst is unsure how to handle such a large-scale remediation effort. Which of the following would be the next logical step?

A. Identify the assets with a high value and remediate all vulnerabilities on those hosts.

B. Perform remediation activities for all critical and high vulnerabilities first.

C. Perform a risk calculation to determine the probability and magnitude of exposure.

D. Identify the vulnerabilities that affect the most systems and remediate them first.

Correct Answer: B

QUESTION 2

A Chief Information Officer wants to implement a BYOD strategy for all company laptops and mobile phones. The Chief Information Security Officer is concerned with ensuring all devices are patched and running some sort of protection against malicious software. Which of the following existing technical controls should a security analyst recommend to best meet all the requirements?

A. EDR

B. Port security

C. NAC

D. Segmentation

Correct Answer: A

EDR stands for endpoint detection and response, which is a type of security solution that monitors and protects all devices that are connected to a network, such as laptops and mobile phones. EDR can help to ensure that all devices are

patched and running some sort of protection against malicious software by providing continuous visibility, threat detection, incident response, and remediation capabilities. EDR can also help to enforce security policies and compliance

requirements across all devices .

https://www.crowdstrike.com/epp-101/what-is-endpoint-detection-and-response-edr/

QUESTION 3

A security analyst is performing vulnerability scans on the network. The analyst installs a scanner appliance, configures the subnets to scan, and begins the scan of the network. Which of the following would be missing from a scan performed with this configuration?

A. Operating system version

B. Registry key values

C. Open ports

D. IP address

Correct Answer: B

QUESTION 4

Which of the following describes how a CSIRT lead determines who should be communicated with and when during a security incident?

A. The lead should review what is documented in the incident response policy or plan

B. Management level members of the CSIRT should make that decision

C. The lead has the authority to decide who to communicate with at any t me

D. Subject matter experts on the team should communicate with others within the specified area of expertise

Correct Answer: A

The incident response policy or plan is a document that defines the roles and responsibilities, procedures and processes, communication and escalation protocols, and reporting and documentation requirements for handling security incidents. The lead should review what is documented in the incident response policy or plan to determine who should be communicated with and when during a security incident, as well as what information should be shared and how. The incident response policy or plan should also be aligned with the organizational policies and legal obligations regarding incident notification and disclosure.

QUESTION 5

A digital forensics investigator works from duplicate images to preserve the integrity of the original evidence. Which of the following types of media are most volatile and should be preserved? (Select two).

A. Memory cache

B. Registry file

C. SSD storage

D. Temporary filesystems

E. Packet decoding

F. Swap volume

Correct Answer: AF

Memory cache and swap volume are types of media that are most volatile and should be preserved during a digital forensics investigation. Volatile media are those that store data temporarily and lose their contents when the power is turned off or interrupted. Memory cache is a small and fast memory that stores frequently used data or instructions for faster access by the processor. Swap volume is a part of the hard disk that is used as an extension of the memory when the memory is full or low . https://www.techopedia.com/definition39/memory-dump