CS0-002$^{Q\&As}$

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-002 Exam with 100% Guarantee

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

https://www.geekcert.com/cs0-002.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A malware infection spread to numerous workstations within the marketing department. The workstations were quarantined and replaced with machines.

Which of the following represents a FINAL step in the eradication of the malware?

A. The workstations should be isolated from the network.

B. The workstations should be donated for reuse.

C. The workstations should be reimaged.

D. The workstations should be patched and scanned.

Correct Answer: D

QUESTION 2

Which of me following BEST articulates the benefit of leveraging SCAP in an organization\\'s cybersecurity analysis toolset?

A. It automatically performs remedial configuration changes lo enterprise security services

B. It enables standard checklist and vulnerability analysis expressions for automaton

C. It establishes a continuous integration environment for software development operations

D. It provides validation of suspected system vulnerabilities through workflow orchestration

Correct Answer: B

QUESTION 3

A security analyst has received a report that servers are no longer able to connect to the network. After many hours of troubleshooting, the analyst determines a Group Policy Object is responsible for the network connectivity issues. Which of the following solutions should the security analyst recommend to prevent an interruption of service in the future?

A. CI/CD pipeline

B. Impact analysis and reporting

C. Appropriate network segmentation

D. Change management process

Correct Answer: D

QUESTION 4

A security analyst is making recommendations for securing access to the new forensic workstation and workspace. Which of the following security measures should the analyst recommend to protect access to forensic data?

A. Multifactor authentication Polarized lens protection Physical workspace isolation

B. Secure ID token Security reviews of the system at least yearly Polarized lens protection

C. Bright lightning in all access areas Security reviews of the system at least yearly Multifactor authentication

D. Two-factor authentication into the building Separation of duties Warning signs placed in clear view

Correct Answer: A

QUESTION 5

A security analyst is investigating malicious traffic from an internal system that attempted to download proxy avoidance software as identified from the firewall logs but the destination IP is blocked and not captured. Which of the following should the analyst do?

A. Shut down the computer

B. Capture live data using Wireshark

C. Take a snapshot

D. Determine if DNS logging is enabled.

E. Review the network logs.

Correct Answer: D

The DNS debug log provides extremely detailed data about all DNS information that is sent and received by the DNS server, similar to the data that can be gathered using packet capture tools such as network monitor.

Latest CS0-002 Dumps CS0-002 PDF Dumps CS0-002 VCE Dumps