EndExam

QUESTION & ANSWER

Accurate study guides, High passing rate!

We offer free update service for one year!

http://www.endexam.com

Exam : **CS0-001**

Title : CompTIA CySA+ Certification Exam

Version : DEMO

1.A cybersecurity analyst has received a report that multiple systems are experiencing slowness as a result of a DDoS attack.
Which of the following would be the BEST action for the cybersecurity analyst to perform?
A. Continue monitoring critical systems.
B. Shut down all server interfaces.
C. Inform management of the incident.
D. Inform users regarding the affected systems.
Answer: C

2.An analyst has received unusual alerts on the SIEM dashboard. The analyst wants to get payloads that the hackers are sending toward the target systems without impacting the business operation.
Which of the following should the analyst implement?
A. Honeypot
B. Jump box
C. Sandboxing
D. Virtualization
Answer: A

3.A reverse engineer was analyzing malware found on a retailer's network and found code extracting track data in memory.
Which of the following threats did the engineer MOST likely uncover?
A. POS malware
B. Rootkit
C. Key logger
D. Ransomware
Answer: A

4.An HR employee began having issues with a device becoming unresponsive after attempting to open an email attachment. When informed, the security analyst became suspicious of the situation, even though there was not any unusual behavior on the IDS or any alerts from the antivirus software.
Which of the following BEST describes the type of threat in this situation?
A. Packet of death
B. Zero-day malware
C. PII exfiltration
D. Known virus
Answer: B

5.Which of the following is MOST effective for correlation analysis by log for threat management?
A. PCAP
B. SCAP
C. IPS
D. SIEM
Answer: D