Comptia
CS0-004
CompTIA Cybersecurity Analyst (CySA+)

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 6.0

Question: 1

In the Diamond Model of Intrusion Analysis, which element represents the target of the attacker?

A. Victim
B. Capability
C. Infrastructure
D. Adversary

Answer: A

Question: 2

A SOC analyst needs to inspect suspicious network packets and identify protocol anomalies during an incident investigation. Which TWO tools are MOST appropriate?
(Choose two.)

A. WHOIS
B. tcpdump
C. VirusTotal
D. Wireshark
E. CyberChef

Answer: B,D

Question: 3

Why is establishing an incident timeline important?

A. It reconstructs attacker activity in chronological order.
B. It calculates software licensing costs.
C. It replaces vulnerability scanning.
D. It documents employee attendance.

Answer: A

Question: 4

Which TWO concepts are associated with identity and access management in security operations? (Choose two.)

A. Packet fragmentation
B. Data deduplication
C. Privileged access management
D. Secrets management
E. Thermal monitoring

Answer: C,D

Question: 5

A vulnerability scanner identifies a library with the following metadata:
Library: Log4j 2.14
Known CVE: Critical
Patch Available: Yes
What should the analyst recommend?

A. Remove endpoint protection
B. Ignore because Java is sandboxed
C. Upgrade to the patched version immediately
D. Disable vulnerability scanning

Answer: C

Question: 6

Which TWO frameworks are commonly referenced during compliance baseline scanning? (Choose two.)

A. CIS Benchmarks
B. WPA3
C. OAuth 2.0
D. DNSSEC
E. ISO/IEC 27001

Answer: A,E

Question: 7

During an incident, the legal department instructs the response team not to delete or alter logs related to a compromised database. What has likely been issued?

A. Risk exception
B. Legal hold
C. Scan waiver
D. Service-level objective

Answer: B

Question: 8

An analyst has the following evidence sources:
Firewall logs
EDR alerts
VPN authentication logs
Database access logs
The incident involves suspected unauthorized database access using stolen VPN credentials. Which TWO evidence sources should be correlated FIRST?
(Choose two.)

A. VPN authentication logs
B. Database access logs
C. Printer maintenance logs
D. HVAC sensor logs
E. Building cafeteria records

Answer: A,B

Question: 9

Your organization cannot immediately patch a critical Internet-facing application because of vendor restrictions. Which sequence provides the BEST temporary risk reduction?

A. Disable logging → Wait for vendor patch
B. Remove vulnerability scanner from the network
C. Ignore alerts until maintenance weekend
D. Implement WAF rules → Restrict access → Monitor exploitation attempts

Answer: D

Question: 10

An organization is developing a threat intelligence program and wants to improve confidence in the intelligence it receives. Which TWO characteristics should analysts evaluate?
(Choose two.)

A. Timeliness
B. Screen resolution
C. Accuracy
D. Network latency
E. Printer availability

Answer: A,C

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/