Passcert

Higher Quality, better service!

Q&A

Http://www.passcert.com

We offer free update service for one year.

Exam : **CS0-004**

Title : CompTIA Cybersecurity Analyst (CySA+) Certification Exam

Version : DEMO

1.Which of the following is the most important reason why tactics, techniques, and procedures (TTP) are beneficial to a defensive strategy?
A. TTP provides useful insights on the hash values and internet protocol addresses attributed to an attacker.
B. TTP provides useful insights on an attacker's indicators of compromise.
C. TTP provides useful insights on the tools used by an attacker.
D. TTP provides useful insights on the strategy and behavior of an attacker.
Answer: D

2.Which of the following is the best reason to heavily segment business-critical assets from within the network?
A. Legacy systems
B. Degraded functionality
C. Asset obfuscation
D. Proprietary server
Answer: A

3.A cybersecurity analyst receives an unstructured text document that contains advanced persistent threat (APT)-related indicators of compromise (IoCs). The analyst needs to extract the IPv4 addresses. Which of the following is the best tool to accomplish this task?
A. CyberChef
B. Wireshark
C. Zeek
D. Open Cyber Threat Intelligence (OpenCTI)
Answer: A

4.Which of the following best describes why operational technology (OT) devices use compensating controls?
A. Industrial control systems use significant network bandwidth.
B. Outage windows are usually scheduled.
C. Traditional IT security solutions may not be compatible.
D. OT devices are typically not encrypted.
Answer: C

5.The Chief Information Security Officer (CISO) reviews the following security operations metrics from the last month:

Metric	Value	Notes
Alerts	3701	Raw SIEM alerts
Investigations	491	Actively investigated events
Incidents	5	Number of times incident was declared
Analyst hours	1400	Hours analysts spent investigating
Junior analysts	4	Total number of junior analysts
Senior analysts	7	Total number of senior analysts

Which of the following is the best action to improve overall security operations efficiency?

A. Leverage a cloud security posture management tool to add asset context to alerts.

B. Analyze and tune the detections that are causing non-actionable alerts.

C. Implement playbooks for the junior analysts to use during investigations.

D. Perform internal incident training on the most common alerts from security information and event management (SIEM).

Answer: B