VirtuLearn
Trusted, Accurate & Reliable

TRUSTED, ACCURATE AND RELIABLE

The most comprehensive IT certification preparation materials in the industry!

Expert-Verified | Exam-Ready | Regularly Updated

https://www.virtulearner.com
support@virtulearner.com

CompTIA

CS0-004

CompTIA CySA+ V4

Exam Topics:

1. Security Operations
2. Vulnerability Management
3. Incident Response and Management
4. Reporting and Communication

Exam Topic: Section: Security Operations

QUESTION: 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(s): D

Explanation:
TTPs describe how an adversary operates. These behavioral patterns are generally more durable and strategically useful for detection and defense than easily changed indicators such as IP addresses, hashes, or tools.

QUESTION: 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(s): A

Explanation:
Legacy systems may be unsupported or unable to receive security patches. Strong network segmentation limits their exposure and prevents attackers from easily reaching them through lateral movement.

QUESTION: 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(s): A

Explanation:
CyberChef can parse unstructured text and extract IPv4 addresses using built-in extraction and regular-expression operations. Wireshark and Zeek analyze network traffic, while OpenCTI manages threat intelligence.

QUESTION: 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(s): C

Explanation:
OT systems often use specialized, legacy, or availability-sensitive equipment that cannot support conventional security tools or patches. Compensating controls provide alternative protection without disrupting operations.

QUESTION: 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.