Comptia
CS0-004
CompTIA Cybersecurity Analyst CySA+ V4 (New Version)

Latest Version: 6.0

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: D

Explanation:
Tactics, techniques, and procedures represent the behavioral characteristics of an adversary rather than merely individual technical artifacts. A tactic describes the adversary's objective, a technique identifies how that objective is achieved, and procedures represent the specific implementation observed during an intrusion. Consequently, TTP intelligence allows defenders to understand how an attacker operates, including patterns of reconnaissance, persistence, privilege escalation, lateral movement, command-and-control activity, and other operational behaviors.
Options A and B focus primarily on indicators of compromise such as IP addresses and hashes. These are useful for detection, but they are comparatively fragile because attackers can replace infrastructure, change domains, regenerate malware, or modify files to produce different hashes. Option C is broader than an individual IoC, but tools can likewise be replaced or modified. Behavioral knowledge is generally more durable because changing established operational methods imposes greater cost on an adversary.
The CS0-004 objectives explicitly place TTPs, Pyramid of Pain, MITRE ATT&CK, attribution, IoC analysis, and behavioral indicators within threat intelligence and threat-hunting concepts.
Study Guide Security Operations → Threat Intelligence and Threat Hunting → TTPs → Pyramid of Pain → MITRE ATT&CK → Behavioral IoCs.

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: A

Explanation:
Legacy systems present a significant security problem because they frequently cannot support current operating systems, security agents, encryption mechanisms, authentication controls, or vendor patches. When a business-critical legacy system cannot be remediated normally, strong network segmentation becomes an important compensating control. The objective is to reduce the system's reachable attack surface and restrict which users, hosts, protocols, and applications can communicate with it.
A segmented legacy asset might be placed in a dedicated VLAN or security zone and protected through restrictive firewall access-control rules, jump hosts, allowlisting, enhanced logging, and continuous monitoring. Even though segmentation does not remove the underlying vulnerability, it decreases exposure and makes exploitation or lateral movement considerably more difficult.
Degraded functionality is generally an effect or remediation constraint rather than the strongest reason for isolation. Asset obfuscation does not provide reliable security because hidden systems can still be discovered through enumeration or traffic analysis. A proprietary server is not automatically vulnerable merely because its implementation is proprietary; it may still support modern patches and security controls.
CS0-004 specifically covers segmentation as a vulnerability-scanning consideration, compensating controls as a mitigation strategy, and legacy systems as an important inhibitor to remediation.
Study Guide Vulnerability Management → Vulnerability Prioritization and Mitigation → Compensating Controls → Segmentation → Legacy-System Constraints.

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: A

Explanation:

CyberChef is the most appropriate option because the task involves parsing and extracting structured indicators from unstructured text, rather than inspecting network traffic or managing a threat-intelligence repository. CyberChef provides operations for text manipulation, pattern matching, regular expressions, decoding, extraction, and transformation. An analyst can therefore feed the document into CyberChef and identify IPv4 address patterns without manually reviewing potentially thousands of characters.
Wireshark is primarily a packet-analysis platform. It would be appropriate if the analyst needed to inspect packets from a PCAP or live network capture, but the scenario provides a text document. Zeek is a network security monitoring and traffic-analysis framework that converts network activity into structured logs; it is similarly unnecessary for static textual extraction.
OpenCTI is a threat-intelligence platform designed to organize, correlate, and manage intelligence objects and relationships. It could store the resulting IoCs after extraction, but it is not the most efficient tool for extracting IPv4 strings from raw text.
The official CS0-004 objectives identify CyberChef under decoding/parsing tools, while Wireshark and Zeek are classified under packet analysis and OpenCTI under threat-intelligence platforms.
Study Guide Security Operations → Tools for Malicious-Activity Analysis → Decoding/Parsing → CyberChef → Pattern Recognition/Regular Expressions → IoC Analysis.

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: C

Explanation:
Operational technology environments frequently contain specialized controllers, industrial control systems, supervisory control and data acquisition equipment, embedded operating systems, and vendor-specific devices that were designed primarily for availability, safety, deterministic operation, and long service life. Traditional enterprise security controls—such as endpoint detection agents, vulnerability scanners, host-based firewalls, aggressive patching mechanisms, or modern authentication software—may not be supported and can potentially interfere with operational processes.
For this reason, organizations often implement compensating controls around OT assets when the preferred security control cannot be deployed directly. Examples include network segmentation, tightly controlled firewall rules, protocol allowlisting, passive monitoring, secure jump servers, access restrictions, enhanced logging, and additional physical controls. These measures reduce risk without requiring unsupported software to be installed on sensitive industrial devices.

High network bandwidth consumption is not the defining reason for compensating controls. Scheduled outage windows can actually facilitate maintenance rather than explain why alternative controls are required. Likewise, lack of encryption may be a weakness in some environments, but it does not explain the broader compatibility problem.
CS0-004 specifically places OT, ICS, and SCADA under critical-infrastructure concepts in Security Operations and separately recognizes compensating controls as a formal vulnerability mitigation strategy.
Study Guide Security Operations → Critical Infrastructure → OT/ICS/SCADA → Security Architecture → Compatibility Constraints and Compensating Controls.

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.
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

Explanation:
The most direct method for improving SOC efficiency when excessive alerts are non-actionable is to identify the detections generating that noise and perform rule and alert tuning. Non-actionable detections consume analyst time, increase queue depth, contribute to alert fatigue, and can obscure genuinely malicious activity. Tuning may include adjusting thresholds, refining correlation logic, adding exclusions for legitimate behavior, improving indicator context, modifying detection conditions, or disabling rules that consistently generate false positives without meaningful security value.

A cloud security posture management platform may improve context for cloud-related findings, but it does not directly correct poorly performing detection logic across the broader SOC.
Playbooks improve consistency and reduce investigation variability, particularly for junior analysts, but they still force personnel to process alerts that should not have been generated.
Training can improve analyst performance, yet it also fails to address the source of excessive non-actionable notifications.
The CS0-004 Security Operations objectives explicitly identify efficiency and process improvement, including standardized processes, automation and orchestration, data enrichment, rule/alert tuning, dashboard creation, and technology integration.
Therefore, the optimal operational improvement is to reduce unnecessary workload at the detection layer itself.
Study Guide Security Operations → Efficiency and Process Improvement → Data Enrichment → Rule/Alert Tuning → SOC Optimization.

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer