DUMPSARENA

CompTIA Cybersecurity Analyst CySA+ V4 (New Version)

CompTIA CS0-004

Version Demo

Total Demo Questions: 9

Total Premium Questions: 93

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Security Operations	41
Topic 2, Vulnerability Management	23
Topic 3, Incident Response Management	21
Topic 4, Reporting and Communication	8
Total	93

QUESTION NO: 1

A SIEM detection for suspicious PowerShell activity is generating false positives from an approved deployment platform. The security team must reduce alert volume without creating a broad monitoring blind spot.

Which of the following alert-tuning changes are the most appropriate? Select two.

A. Exclude the verified deployment service account and signed approved script path.

B. Require additional suspicious execution characteristics in the detection logic.

C. Exclude all PowerShell activity from the detection rule.

D. Disable the detection rule until the deployment platform is replaced.

E. Increase the alert threshold without reviewing the benign execution pattern.

ANSWER: A B

Explanation:

A narrowly scoped exclusion for the verified deployment service account and signed approved script path reduces known benign alerts while preserving detection for other PowerShell activity. Adding contextual conditions, such as suspicious encoded commands, unexpected parent processes, or execution from user-writable locations, improves detection fidelity by focusing on behaviors associated with abuse.

Excluding all PowerShell activity or disabling the rule would create significant visibility gaps because PowerShell is frequently used by attackers. Raising the alert threshold without understanding the benign pattern can suppress true positives along with false positives.

QUESTION NO: 2 - (SIMULATION)

A systems administrator is reviewing the output of a vulnerability scan.

INSTRUCTIONS -

Review the information in each tab.

Based on the organization’s environment architecture and remediation standards, select the server to be patched within 14 days and select the appropriate technique and mitigation.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Vulnerability remediation timeframes | Environment | Output

CVSS risk level	Standard	Applies to OPS	TEST	STAGE
CVSS > 9.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **7 calendar days**	✔	✔	✘
CVSS > 7.9 < 9.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **14 calendar days**	✔	✘	✘
CVSS > 5.0 < 7.9	Must be patched or remediated and verified by a subsequent vulnerability scan within **30 calendar days**	✔	✘	✘
CVSS > 0 < 5.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **60 calendar days**	✔	✘	✘

Any of these timeframes may be accelerated at the discretion of the Chief Information Security Officer (CISO).

- If patching cannot be completed or a vendor has not made a patch available within the timeframe in the table outlined above, compensating controls must be put in place within the timeframes listed above and the exception process must be followed.
- If a patch requires a reboot for installation, the reboot must occur within the timeframes outlined above.
- All mitigations must be tested in the lower environments before being promoted to operations.
- Appropriate risk management processes should be considered when an applicable timeframe is not required for an environment.

Vulnerability remediation timeframes | Environment | Output

Environment name	Environment location	Subnets	Domain	Publicly accessible	NGFW	Load balancer	MFA required
ops.comptia.org	External	203.17.18.20 203.17.18.30 192.168.60.0/24 192.168.61.0/24	comptia.org	Yes	Yes	Yes	No
stage.comptia.org	Internal	192.168.76.0/24 192.168.75.0/24	comptia.org	No	No	Yes	Yes
test.comptia.org	External	192.168.50.0/24 192.168.51.0/24	comptia.org	No	Yes	Yes	Yes

Vulnerability remediation timeframes | Environment | Output

Title:	Microsoft IIS: Unsupported software version detected
Description:	The software version detected is no longer supported.
Affected asset:	192.168.76.50
Risk:	Unpatched software
Reference:	CVE-2022-0155, CVSS 9.2
Title:	Sensitive cookie in HTTPS session without "secure" attribute
Description:	The secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over HTTP session.
Affected asset:	192.168.76.60
Risk:	Session sidejacking
Reference:	CVE-2021-0462, CVSS 7.4
Title:	Untrusted SSL/TLS Server X.509 certificate
Description:	The server's TLS/SSL certificate is signed by a certificate authority that is untrusted or unknown.
Affected asset:	192.168.51.32
Risk:	May allow on-path attackers to insert a spoofed certificate for any distinguished name (DN).
Reference:	CVE-2021-1234, CVSS 8.1
Title:	Sensitive cookie in HTTPS session without "secure" attribute
Description:	The secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over HTTP session.
Affected asset:	192.168.60.45
Risk:	Session sidejacking
Reference:	CVE-2021-0462, CVSS 7.4
Title:	Web server is susceptible to TLS downgrade attacks
Description:	The server permits the web client to select and use its own preferences.
Affected asset:	192.168.60.90
Risk:	May allow data to be vulnerable.
Reference:	CVE-2021-1234, CVSS 8.1
Title:	Basic authentication
Description:	Website is configured to permit use of `.htaccess` files on directories.
Affected asset:	192.168.51.90
Risk:	May allow privileged access to sensitive data.
Reference:	CVE-2021-38361, CVSS 5.1

Answer Area

Select the server to be patched within 14 calendar days:

- ☐ 192.168.51.32
- ☐ 192.168.76.50
- ☐ 192.168.76.60
- ☐ 192.168.60.45
- ☐ 192.168.60.90
- ☐ 192.168.51.90

Select the appropriate technique and mitigation:

Select

- Select
- Compensating control; implement secure session tokens
- Compensating control; create new ACL on firewall to block port 443
- Compensating control; implement MFA on the application
- Reconfigure; transition to a new identity and access manager
- Request exception; organization needs time to procure a PKI
- Reconfigure; restrict to use only modern cipher suites
- Reconfigure; upgrade IIS to current release
- Request exception; legacy protocol could have operational impact

ANSWER: See the explanation for the answer

Explanation:

Select: `192.168.76.50`

Select technique and mitigation: `Reconfigure; upgrade IIS to current release`

QUESTION NO: 3

An incident response team identifies a malicious uniform resource locator (URL) associated with a required business process and performs the following activities:

• Access to the URL has been restricted only to the necessary users through firewall rules and Cloud Security Group rules.

• Additional monitoring has been enabled for traffic related to that site and the allowed users.

• All application servers that need to access that site have been patched with the latest security and software updates.

• Application owners have been notified of the severity and need to remediate this reported issue.

Which of the following best describes the overall mitigation the security team is performing?

A. Patching solutions

B. Configuration management

C. Compensating controls

D. Attack surface management

ANSWER: C

Explanation:

Compensating controls is correct because the organization must retain limited access to a known malicious URL to support a required business process, rather than applying the preferred safeguard of completely blocking it. The security team therefore applies alternative, layered measures that reduce the likelihood and impact of compromise while allowing the necessary activity to continue. Restricting access to specifically authorized users through firewall and cloud security-group rules limits exposure and implements segmentation. Increasing monitoring creates greater visibility into activity involving the URL and the users permitted to reach it, enabling faster detection and response if suspicious behavior occurs. Patching the application servers reduces the chance that a malicious site could successfully exploit a known weakness in a system that must communicate with it.

These measures do not eliminate the underlying risk created by the required connection; instead, they provide safeguards that are appropriate when full removal of the risk is not operationally feasible. This is the central purpose of compensating controls in risk treatment: maintaining necessary business functionality while establishing alternative protections that achieve an acceptable level of security. The remediation notification to application owners further supports eventual correction of the business dependency. CompTIA includes compensating controls among relevant security-control and vulnerability-mitigation concepts in the CySA+ objectives. See the CompTIA exam objectives resource and NIST's Security and Privacy Controls guidance.

QUESTION NO: 4

An analyst reviews the following log entries:

Time (UTC)	Source Internet Protocol (IP)	Source hostname	Source port/protocol	Destination IP	Destination port/protocol
16:44:53	192.168.1.57	ws-57	49571/client	192.168.1.2	22/ssh
16:44:54	192.168.1.57	ws-57	44236/client	192.168.1.2	23/telnet
16:44:55	192.168.1.57	ws-57	46871/client	192.168.1.2	80/http
16:44:56	192.168.1.57	ws-57	43664/client	192.168.1.2	139/netbios
16:44:57	192.168.1.57	ws-57	50127/client	192.168.1.2	443/https
16:44:58	192.168.1.57	ws-57	48741/client	192.168.1.2	445/smb
16:44:59	192.168.1.57	ws-57	50111/client	192.168.1.2	3389/rdp
16:46:33	192.168.1.2	dc-1	445/smb	192.168.1.57	48741/client
16:52:12	192.168.1.57	ws-57	49853/client	185.167.3.24	53/https
16:59:31	192.168.1.57	ws-57	49953/client	192.168.1.25	25/smtp

Which of the following conclusions should the analyst reach? (Choose two.)

A. Host ws-57 is performing a network scan against dc-1.

B. Domain Controller dc-1 is performing a network scan against ws-57.

C. Host ws-57 delivered a phishing email via Simple Mail Transfer Protocol.

D. Host ws-57 is communicating on a service using a non-standard port.

E. Domain Controller dc-1 is infected with ransomware and initiating connections with ws-57.

F. Domain Controller dc-1 is communicating using a non-standard port.

ANSWER: A D

Explanation:

The evidence supports the conclusions that **Host ws-57 is performing a network scan against dc-1.** and **Host ws-57 is communicating on a service using a non-standard port.** The connection pattern identifies ws-57 as the initiating source and dc-1 as the destination. Multiple connection attempts from one host toward different destination ports on the same target over a limited interval are a common network-log indicator of port scanning or service enumeration. This activity is used to discover reachable services and their exposure before possible follow-on activity. NIST describes scanning as a technique for identifying hosts, open ports, and services during security testing and assessment; the same traffic characteristics are valuable for detection analysis. See NIST SP 800-115.

The port and service information also indicates that ws-57 is using a service on a port other than that service's conventional registered port. Analysts should validate service identity using available protocol or application information rather than assuming that a port number alone definitively identifies the service. Comparing the observed port/service relationship against registered service assignments, such as those maintained in the IANA Service Name and Port Number Registry, provides the baseline needed to recognize this non-standard usage.

QUESTION NO: 5

An incident response analyst has acquired a forensic disk image from a potentially compromised server. The organization expects that the image may be used in legal proceedings.

Which of the following actions should the analyst take to preserve the image's integrity and traceability? Select two.

A. Calculate and record a cryptographic hash of the forensic image.

B. Maintain a chain-of-custody record for each evidence transfer.

C. Perform all analysis directly against the original forensic image.

D. Store the image in an unrestricted shared network location.

E. Rename the image file without documenting the change.

ANSWER: A B

Explanation:

Calculating and recording a cryptographic hash for the acquired image provides a means to verify that the evidence has not changed. Maintaining a chain-of-custody record documents each transfer, handler, date, time, and purpose, establishing accountability and traceability.

Working directly from the original image increases the chance of altering or corrupting the evidence; analysts should use verified working copies. Storing the image in a shared location without access restrictions weakens custody controls. Renaming the file without documenting the change can create confusion and does not demonstrate integrity.

QUESTION NO: 6

Based on recent alerts, a security analyst thinks a web application server was compromised. The analyst reviews the following server output:

```
09:59:57 up 1:19, 4 users, load average: 2.01, 0.75, 0.27
USER     TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
comptia  -        0.0.0.0         09:28    29:28  0.00s  0.03s  gdm-session-worker
www      tty2     89.123.222.5    03:28    25:28  0.00s  0.03s  /var/www/apache2
gdm      tty1     -               08:38    1:19   5.80s  0.09s  /usr/bin/gjs
comptia2 -        0.0.0.0         09:25    39:09  0.05s  0.09s  gdm-session-worker
```

Which of the following best describes what has occurred?

A. An initiated unauthorized session

B. Too many users logged in at the same time

C. High resource consumption

D. Abnormal idle times for each user

ANSWER: A

Explanation:

An initiated unauthorized session is the best description because the server output indicates that an interactive user session has been established on the web application server. In an incident context, an unexpected login or terminal session is a significant indicator of compromise: attackers who exploit a web-facing application commonly establish an interactive shell or remote session to execute commands, explore the host, elevate privileges, and maintain persistence. Session-reporting output can reveal the account associated with the session, its terminal, its source host or address, the login time, and the currently running command. Those details allow the analyst to validate whether the access was expected and attributable to an authorized administrator or service workflow. The immediate response should include preserving relevant evidence, such as authentication logs, process information, network connections, and the displayed session details, before terminating access if organizational incident-response procedures permit. Linux utilities used to inspect logged-in users and their active processes are documented in the w(1) manual page and the who(1) manual page. These utilities are particularly useful for identifying unexpected interactive access during triage.

QUESTION NO: 7

Which of the following is the main concept behind the use of an attack methodology framework?

A. Implementing continuous monitoring and rapid deployment of system fixes over the traditional patch, test, and deploy approach

B. Prioritizing vulnerabilities that can be exploited based on risk calculations and using the consequences and likelihood of the exploits to determine where resources should be allocated

C. Approaching cybersecurity from the perspective of a threat actor and using their common behaviors and motivations to identify secure solutions

D. Applying a Zero Trust environment by assuming networks and systems are vulnerable to malicious actions by both external, hostile adversaries and insider threats

ANSWER: C

Explanation:

Approaching cybersecurity from the perspective of a threat actor and using their common behaviors and motivations to identify secure solutions is the main concept behind an attack methodology framework. These frameworks organize adversary activity into recognizable tactics, techniques, and procedures, allowing defenders to think through how an attacker might achieve objectives such as gaining initial access, escalating privileges, moving laterally, or exfiltrating data. This attacker-centered view helps a security team assess whether its current controls provide meaningful coverage, identify detection gaps, and develop threat-hunting hypotheses based on realistic behaviors rather than isolated indicators. For example, a team can map observed telemetry and security controls to known adversary techniques, then prioritize additional logging, detections, or mitigations where coverage is limited. The MITRE ATT&CK knowledge base is a widely used example: it documents adversary tactics and techniques based on real-world observations and supports defensive activities including threat modeling, detection engineering, and gap analysis. CompTIA CySA+ similarly expects analysts to use frameworks and intelligence to understand attacker behavior and improve monitoring and response. See the MITRE ATT&CK knowledge base and CompTIA's CySA+ certification overview.

QUESTION NO: 8

An analyst uses an AI platform to help correlate events. The AI output contains events that did not happen. This results in inaccurate correlations.

Which of the following best describes what has occurred?

A. Hallucinations

B. Data exposure

C. Malicious prompts

D. Model poisoning

ANSWER: A

Explanation:

Hallucinations is correct because the AI platform has generated events that are not supported by the underlying logs, telemetry, or other evidence. In an AI context, a hallucination is output that may appear plausible and confident but is fabricated, inaccurate, or ungrounded in the source data. When used for security-event correlation, this can introduce false relationships, misstate the sequence of activity, and lead an analyst to investigate incidents that did not occur. The key characteristic in this scenario is the creation of nonexistent events, rather than merely a formatting or correlation error. AI-generated correlation should therefore be treated as decision support and validated against authoritative sources such as SIEM records, endpoint telemetry, network logs, and case evidence before it drives triage, containment, or reporting decisions. NIST describes confabulation, commonly called hallucination, as the generation of false or erroneous content presented as factual. Its guidance emphasizes evaluating and managing this risk when generative AI is used in consequential workflows, including cybersecurity operations. See the NIST AI 600-1 Generative AI Profile and NIST's AI Risk Management Framework resources.

QUESTION NO: 9

A cloud monitoring platform detects unusual API activity from a service identity used by a production application. The identity created new access credentials and enumerated multiple storage locations outside its normal activity pattern. The application must remain available while the incident is investigated.

Which of the following actions should the incident response team take to contain the incident and determine its scope? Select two.

A. Remove all role assignments from every cloud service identity.

B. Delete cloud audit logs to prevent unauthorized access to them.

C. Create replacement credentials for the application and revoke the suspected credentials.

D. Review cloud audit logs for activity associated with the service identity and newly created credentials.

E. Restore the affected storage locations from backup immediately.

ANSWER: C D

Explanation:

The team should create and deploy replacement credentials for the production application, then revoke the suspected credentials. This removes the attacker’s likely access path while preserving the application’s required functionality. Simply disabling the service identity without a replacement credential could create an unnecessary production outage.

The team should also review cloud audit logs for activity associated with the service identity and any newly created credentials. Audit records can identify the source locations, API actions, accessed resources, privilege changes, and additional identities involved. Deleting logs would destroy evidence, while removing every role assignment before analysis could disrupt legitimate services without establishing the incident scope.