Vendor: CompTIA

Exam Code:CS0-002

Exam Name: CompTIA Cybersecurity Analyst (CySA+)

Version: Demo

QUESTION 1

A security analyst is researching an incident and uncovers several details that may link to other incidents. The security analyst wants to determine if other incidents are related to the current incident

Which of the following threat research methodologies would be MOST appropriate for the analyst to use?

A. Reputation data

B. CVSS score

C. Risk assessment

D. Behavioral analysis

Correct Answer: D

QUESTION 2

Which of the following would a security engineer recommend to BEST protect sensitive system data from being accessed on mobile devices?

A. Use a UEFl boot password.

B. Implement a self-encrypted disk.

C. Configure filesystem encryption

D. Enable Secure Boot using TPM

Correct Answer: C

QUESTION 3

A medical organization recently started accepting payments over the phone. The manager is concerned about the impact of the storage of different types of data. Which of the following types of data incurs the highest regulatory constraints?

A. PHI

B. PCI

C. PII

D. IP

Correct Answer: B

QUESTION 4

Which of the following is the BEST option to protect a web application against CSRF attacks?

A. Update the web application to the latest version.

B. Set a server-side rate limit for CSRF token generation.

C. Avoid the transmission of CSRF tokens using cookies.

D. Configure the web application to only use HTTPS and TLS 1.3.

Correct Answer: C

CSRF tokens are random values that are generated by the server and included in requests that perform state-changing actions. They are used to prevent CSRF attacks by verifying that the request originates from a legitimate source.

However, if the CSRF tokens are transmitted using cookies, they are vulnerable to being stolen or forged by an attacker who can exploit other vulnerabilities, such as cross-site scripting (XSS) or cookie injection. Therefore, a better option is to

avoid the transmission of CSRF tokens using cookies and use other methods, such as hidden form fields or custom HTTP headers. References:

CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 11; https://owasp.org/www-community/attacks/csrf

---

QUESTION 5

While reviewing proxy logs, the security analyst noticed a suspicious traffic pattern. Several internal hosts were observed communicating with an external IP address over port 80 constantly. An incident was declared, and an investigation was launched. After interviewing the affected users, the analyst determined the activity started right after deploying a new graphic design suite. Based on this information, which of the following actions would be the appropriate NEXT step in the investigation?

A. Update all antivirus and anti-malware products, as well as all other host-based security software on the servers the affected users authenticate to.

B. Perform a network scan and identify rogue devices that may be generating the observed traffic. Remove those devices from the network.

C. Identify what the destination IP address is and who owns it, and look at running processes on the affected hosts to determine if the activity is malicious or not.

D. Ask desktop support personnel to reimage all affected workstations and reinstall the graphic design suite. Run a virus scan to identify if any viruses are present.

Correct Answer: C

QUESTION 6

A recent audit included a vulnerability scan that found critical patches released 60 days prior were not applied to servers in the environment. The infrastructure team was able to isolate the issue and determined it was due to a service being

disabled on the server running the automated patch management application. Which of the following would be the MOST efficient way to avoid similar audit findings in the future?

A. Implement a manual patch management application package to regain greater control over the process.

B. Create a patch management policy that requires all servers to be patched within 30 days of patch release.

C. Implement service monitoring to validate that tools are functioning properly.

D. Set services on the patch management server to automatically run on start-up.

Correct Answer: D

QUESTION 7

The SOC has received reports of slowness across all workstation network segments. The currently installed antivirus has not detected anything, but a different anti-malware product was just downloaded and has revealed a worm is spreading

Which of the following should be the NEXT step in this incident response?

A. Enable an ACL on all VLANs to contain each segment

B. Compile a list of loCs so the IPS can be updated to halt the spread.

C. Send a sample of the malware to the antivirus vendor and request urgent signature creation.

D. Begin deploying the new anti-malware on all uninfected systems.

Correct Answer: D

QUESTION 8

A code review reveals a web application is using time-based cookies for session management. This is a security concern because time-based cookies are easy to:

A. parameterize.

B. decode.

C. guess.

D. decrypt.

Correct Answer: B

QUESTION 9

Bootloader malware was recently discovered on several company workstations. All the workstations run Windows and

are current models with UEFI capability. Which of the following UEFI settings is the MOST likely cause of the infections?

A. Compatibility mode

B. Secure boot mode

C. Native mode

D. Fast boot mode

Correct Answer: A

QUESTION 10

A security analyst at a small regional bank has received an alert that nation states are attempting to infiltrate financial institutions via phishing campaigns. Which of the following techniques should the analyst recommend as a proactive measure to defend against this type of threat?

A. Honeypot

B. Location-based NAC

C. System isolation

D. Mandatory access control

E. Bastion host

Correct Answer: B

QUESTION 11

An organization has the following risk mitigation policies

Risks without compensating controls will be mitigated first if the risk value is greater than $50,000.

Other risk mitigation will be prioritized based on risk value.

The following risks have been identified:

Risk	Probability	Impact	Compensating control?
A	80%	$100,000	Y
B	20%	$500,000	Y
C	50%	$120,000	N
D	40%	$80,000	N

Which of the following is the order of priority for risk mitigation from highest to lowest?

A. A, C, D, B

B. B, C, D, A

C. C, B, A, D

D. C. D, A, B

E. D, C, B, A

Correct Answer: C

QUESTION 12

Which of me following are reasons why consumer IoT devices should be avoided in an enterprise environment? (Select TWO)

A. Message queuing telemetry transport does not support encryption.

B. The devices may have weak or known passwords.

C. The devices may cause a dramatic Increase in wireless network traffic.

D. The devices may utilize unsecure network protocols.

E. Multiple devices may interface with the functions of other loT devices.

F. The devices are not compatible with TLS 12.

Correct Answer: BD