CS0-003 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/cs0-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

An organization has established a formal change management process after experiencing several critical system failures over the past year. Which of the following are key factors that the change management process will include in order to reduce the impact of system failures? (Select two).

A. Ensure users the document system recovery plan prior to deployment.

B. Perform a full system-level backup following the change.

C. Leverage an audit tool to identify changes that are being made.

D. Identify assets with dependence that could be impacted by the change.

E. Require diagrams to be completed for all critical systems.

F. Ensure that all assets are properly listed in the inventory management system.

Correct Answer: DF

The correct answers for key factors in the change management process to reduce the impact of system failures are:

Identify assets with dependence that could be impacted by the change:

This is crucial in change management because understanding the interdependencies among assets can help anticipate and mitigate the potential cascading effects of a change. By identifying these dependencies, the organization can plan

more effectively for changes and minimize the risk of unintended consequences that could lead to system failures.

Ensure that all assets are properly listed in the inventory management system:

Maintaining an accurate and comprehensive inventory of assets is fundamental in change management. Knowing exactly what assets the organization possesses and their characteristics allows for better planning and impact analysis when

changes are made. This ensures that no critical component is overlooked during the change process, reducing the risk of failures due to incomplete information.

Other Options:

Ensure users document system recovery plan prior to deployment: While documenting a system recovery plan is important, it\\'s more related to disaster recovery and business continuity planning than directly reducing the impact of system

failures due to changes.

Perform a full system-level backup following the change: While backups are essential, they are generally a reactive measure to recover from a failure, rather than a proactive measure to reduce the impact of system failures in the first place.

Leverage an audit tool to identify changes that are being made: While using an audit tool is helpful for tracking changes and ensuring compliance, it is not directly linked to reducing the impact of system failures due to changes.

Require diagrams to be completed for all critical systems: While having diagrams of critical systems is useful for understanding and managing them, it is not a direct method for reducing the impact of system failures due to

changes.Diagrams

are more about documentation and understanding rather than proactive change management.

QUESTION 2

An incident response team finished responding to a significant security incident. The management team has asked the lead analyst to provide an after-action report that includes lessons learned. Which of the following is the most likely reason to include lessons learned?

A. To satisfy regulatory requirements for incident reporting

B. To hold other departments accountable

C. To identify areas of improvement in the incident response process

D. To highlight the notable practices of the organization\\'s incident response team

Correct Answer: C

The most likely reason to include lessons learned in an after-action report is to identify areas of improvement in the incident response process. The lessons learned process is a way of reviewing and evaluating the incident response activities and outcomes, as well as identifying and documenting any strengths, weaknesses, gaps, or best practices. Identifying areas of improvement in the incident response process can help enhance the security posture, readiness, or capability of the organization for future incidents, as well as provide feedback or recommendations on how to address any issues or challenges.

QUESTION 3

A security administrator needs to import PII data records from the production environment to the test environment for testing purposes. Which of the following would best protect data confidentiality?

A. Data masking

B. Hashing

C. Watermarking

D. Encoding

Correct Answer: A

Reference: https://aws.amazon.com/what-is/data-masking/#:~:text=Data%20masking%20creates%20fake%20versions,access%20to%20the%20original%20dataset

QUESTION 4

A security analyst performs a weekly vulnerability scan on a network that has 240 devices and receives a report with 2.450 pages. Which of the following would most likely decrease the number of false positives?

A. Manual validation

B. Penetration testing

C. A known-environment assessment

D. Credentialed scanning

Correct Answer: D

Credentialed scanning is a method of vulnerability scanning that uses valid user credentials to access the target systems and perform a more thorough and accurate assessment of their security posture. Credentialed scanning can help to reduce the number of false positives by allowing the scanner to access more information and resources on the systems, such as configuration files, registry keys, installed software, patches, and permissions . https://www.tenable.com/blog/credentialed-vulnerability-scanning-what-why-and-how

QUESTION 5

An analyst is investigating a phishing incident and has retrieved the following as part of the investigation:

cmd.exe /c c:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -NoLogo -NoProfile -EncodedCommand

Which of the following should the analyst use to gather more information about the purpose of this command?

A. Echo the command payload content into \\'base64 -d\\'.

B. Execute the command from a Windows VM.

C. Use a command console with administrator privileges to execute the code.

D. Run the command as an unprivileged user from the analyst workstation.

Correct Answer: A

The command in question involves an encoded PowerShell command, which is typically used by attackers to obfuscate malicious scripts. To decode and understand the payload, one would need to decode the base64 encoded string. This is why option A is the correct answer, as \\'base64 -d\\' is a command used to decode data encoded with base64. This process will reveal the plaintext of the encoded command, which can then be analyzed to understand the actions that the attacker was attempting to perform. Option B is risky and not advised without a controlled and isolated environment. Option C is not safe because executing unknown or suspicious code with administrator privileges could cause harm to the system or network. Option D also poses a risk of executing potentially harmful code on an analyst\\'s workstation.

QUESTION 6

Which of the following is the most appropriate action a security analyst to take to effectively identify the most security risks associated with a locally hosted server?

A. Run the operating system update tool to apply patches that are missing.

B. Contract an external penetration tester to attempt a brute-force attack.

C. Download a vendor support agent to validate drivers that are installed.

D. Execute a vulnerability scan against the target host.

Correct Answer: D

A vulnerability scan is a process of identifying and assessing the security weaknesses of a system or network. A vulnerability scan can help a security analyst to effectively identify the most security risks associated with a locally hosted server, such as missing patches, misconfigurations, outdated software, or exposed services. A vulnerability scan can also provide recommendations on how to remediate the identified vulnerabilities and improve the security posture of the server12 References: 1: What is a Vulnerability Scan? | Definition and Examples 2: Securing a server: risks, challenges and best practices - Vaadata

QUESTION 7

A recent vulnerability scan resulted in an abnormally large number of critical and high findings that require patching. The SLA requires that the findings be remediated within a specific amount of time. Which of the following is the best approach to ensure all vulnerabilities are patched in accordance with the SLA?

A. Integrate an IT service delivery ticketing system to track remediation and closure

B. Create a compensating control item until the system can be fully patched

C. Accept the risk and decommission current assets as end of life

D. Request an exception and manually patch each system

Correct Answer: A

Reference: https://phoenix.security/using-slas-for-better-vulnerability-management-remediation-improving-developers-workflow/

QUESTION 8

A security analyst is reviewing the following log entries to identify anomalous activity:

```
GET https://comptia.org/admin/login.html&user&password\ HTTP/1.1
GET http://comptia.org/index.php\ HTTP/1.1
GET http://comptia.org/scripts/..%5c../Windows/System32/cmd.exe?/C+dir+c:\ HTTP/1.1
GET http://comptia.org/media/contactus.html\ HTTP/1.1
```

Which of the following attack types is occurring?

A. Directory traversal

B. SQL injection

C. Buffer overflow

D. Cross-site scripting

Correct Answer: A

A directory traversal attack is a type of web application attack that exploits insufficient input validation or improper configuration to access files or directories that are outside the intended scope of the web server. The log entries given in

the question show s" sequences in the URL, which indicate an attempt to move up one level in the directory structure. For "" tries to access the /etc/passwd file, which contains user account information on Linux systems. If successful, this attack could allow an attacker to read, modify, or execute files on the web server that are not meant to be accessible.

QUESTION 9

Which of the following is the greatest security concern regarding ICS?

A. The involved systems are generally hard to identify.

B. The systems are configured for automatic updates, leading to device failure.

C. The systems are oftentimes air gapped, leading to fileless malware attacks.

D. Issues on the systems cannot be reversed without rebuilding the systems.

Correct Answer: C

QUESTION 10

Which of the following best describes the goal of a disaster recovery exercise as preparation for possible incidents?

A. To provide metrics and test continuity controls

B. To verify the roles of the incident response team

C. To provide recommendations for handling vulnerabilities

D. To perform tests against implemented security controls

Correct Answer: A

A disaster recovery exercise is a simulation or a test of the disaster recovery plan, which is a set of procedures and resources that are used to restore the normal operations of an organization after a disaster or a major incident. The goal of a disaster recovery exercise is to provide metrics and test continuity controls, which are the measures that ensure the availability and resilience of the critical systems and processes of an organization. A disaster recovery exercise can help evaluate the effectiveness, efficiency, and readiness of the disaster recovery plan, as well as identify and address any gaps or issues . The other options are not the best descriptions of the goal of a disaster recovery exercise. Verifying the roles of the incident response team (B) is a goal of an incident response exercise, which is a simulation or a test of the incident response plan, which is a set of procedures and roles that are used to detect, contain, analyze, and remediate an incident. Providing recommendations for handling vulnerabilities ?is a goal of a vulnerability assessment, which is a process of identifying and prioritizing the weaknesses and risks in an organization\\'s systems or network. Performing tests against implemented security controls (D) is a goal of a penetration test, which is an authorized and simulated attack on an organization\\'s systems or network to evaluate their security posture and identify any vulnerabilities or misconfigurations.

QUESTION 11

A SOC manager receives a phone call from an upset customer. The customer received a vulnerability report two hours ago: but the report did not have a follow-up remediation response from an analyst. Which of the following documents should the SOC manager review to ensure the team is meeting the appropriate contractual obligations for the

customer?

A. SLA

B. MOU

C. NDA

D. Limitation of liability

Correct Answer: A

SLA stands for service level agreement, which is a contract or document that defines the expectations and obligations between a service provider and a customer regarding the quality, availability, performance, or scope of a service. An SLA may also specify the metrics, penalties, or remedies for measuring or ensuring compliance with the agreed service levels. An SLA can help the SOC manager review if the team is meeting the appropriate contractual obligations for the customer, such as response time, resolution time, reporting frequency, or communication channels.

QUESTION 12

During an incident response procedure, a security analyst acquired the needed evidence from the hard drive of a compromised machine. Which of the following actions should the analyst perform NEXT to ensure the data integrity of the evidence?

A. Generate hashes for each file from the hard drive.

B. Create a chain of custody document.

C. Determine a timeline of events using correct time synchronization.

D. Keep the cloned hard drive in a safe place.

Correct Answer: A

QUESTION 13

There are several reports of sensitive information being disclosed via file sharing services. The company would like to improve its security posture against this threat. Which of the following security controls would best support the company in this scenario?

A. Implement step-up authentication for administrators

B. Improve employee training and awareness

C. Increase password complexity standards

D. Deploy mobile device management

Correct Answer: B

The best security control to implement against sensitive information being disclosed via file sharing services is to improve employee training and awareness. Employee training and awareness can help educate employees on the risks and consequences of using file sharing services for sensitive information, as well as the policies and procedures for

handling such information securely and appropriately. Employee training and awareness can also help foster a security culture and encourage employees to report any incidents or violations of information security.

QUESTION 14

The Chief Executive Officer (CEO) has notified that a confidential trade secret has been compromised. Which of the following communication plans should the CEO initiate?

A. Alert department managers to speak privately with affected staff.

B. Schedule a press release to inform other service provider customers of the compromise.

C. Disclose to all affected parties in the Chief Operating Officer for discussion and resolution.

D. Verify legal notification requirements of PII and SPII in the legal and human resource departments.

Correct Answer: D

When a confidential trade secret has been compromised, it\\'s crucial to first verify any legal notification requirements, especially if the compromised information includes Personally Identifiable Information (PII) or Sensitive Personal Identifiable Information (SPII). This step ensures that the organization complies with relevant laws and regulations, which may mandate specific actions or disclosures. Involving the legal and human resources departments helps to ensure that the response is both legally compliant and appropriately managed from an internal perspective.

QUESTION 15

Which of the following BEST explains the function of a managerial control?

A. To scope the security planning, program development, and maintenance of the security life cycle

B. To guide the development of training, education, security awareness programs, and system maintenance

C. To implement data classification, risk assessments, security control reviews, and contingency planning

D. To ensure tactical design, selection of technology to protect data, logical access reviews, and the implementation of audit trails

Correct Answer: C

https://www.examtopics.com/discussions/comptia/view/84935-exam-cs0-002-topic-1-question-191-discussion/