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.leads4pass.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

A product manager is working with an analyst to design a new application that will perform as a data analytics platform and will be accessible via a web browser. The product manager suggests using a PaaS provider to host the application. Which of the following is a security concern when using a PaaS solution?

A. The use of infrastructure-as-code capabilities leads to an increased attack surface.

B. Patching the underlying application server becomes the responsibility of the client.

C. The application is unable to use encryption at the database level.

D. Insecure application programming interfaces can lead to data compromise.

Correct Answer: D

Insecure application programming interfaces (APIs) can lead to data compromise when using a PaaS solution. APIs are interfaces that allow applications to communicate with each other and with the underlying platform. APIs can expose sensitive data or functionality to unauthorized or malicious users if they are not properly designed, implemented, or secured. Insecure APIs can result in data breaches, denial of service, unauthorized access, or code injection . https://spot.io/ resources/cloud-security/paas-security-threats-solutions-and-bestpractices/

QUESTION 2

A vulnerability management team is unable to patch all vulnerabilities found during their weekly scans. Using the third-party scoring system described below, the team patches the most urgent vulnerabilities:

Metric	Description
Cobain	Exploitable by malware
Grohl	Externally facing
Novo	Exploit PoC available
Smear	Older than 2 years
Channing	Vulnerability research activity

Additionally, the vulnerability management team feels that the metrics Smear and Channing are less important than the others, so these will be lower in priority. Which of the following vulnerabilities should be patched first, given the above third-party scoring system?

A. InLoud: Cobain: Yes Grohl: No Novo: Yes Smear: Yes

Channing: No

B. TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No

C. ENameless: Cobain: Yes Grohl: No Novo: Yes Smear: No Channing: No

D. PBleach: Cobain: Yes Grohl: No Novo: No Smear: No Channing: Yes

Correct Answer: B

The vulnerability that should be patched first, given the above third-party scoring system, is:

TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No This vulnerability has three out of five metrics marked as Yes, which indicates a high severity level. The metrics Cobain, Grohl, and Novo are more important than Smear

and Channing, according to the vulnerability management team. Therefore, this vulnerability poses a greater risk than the other vulnerabilities and should be patched first.

QUESTION 3

Which of the following actions would an analyst most likely perform after an incident has been investigated?

A. Risk assessment

B. Root cause analysis

C. Incident response plan

D. Tabletop exercise

Correct Answer: B

After an incident has been investigated, one of the most important actions is to perform a root cause analysis. Root cause analysis helps in identifying the underlying reasons or factors that led to the incident in the first place. By understanding the root causes, organizations can implement corrective actions to prevent similar incidents from occurring in the future. This analysis is crucial for improving the overall security posture and resilience of the organization.

Reference: https://www.ibm.com/topics/incident-response

QUESTION 4

Which of the following best describes the key elements of a successful information security program?

A. Business impact analysis, asset and change management, and security communication plan

B. Security policy implementation, assignment of roles and responsibilities, and information asset classification

C. Disaster recovery and business continuity planning, and the definition of access control requirements and human resource policies

D. Senior management organizational structure, message distribution standards, and procedures for the operation of

security management systems

Correct Answer: B

A successful information security program consists of several key elements that align with the organization\\'s goals and objectives, and address the risks and threats to its information assets. Security policy implementation: This is the process of developing, documenting, and enforcing the rules and standards that govern the security of the organization\\'s information assets. Security policies define the scope, objectives, roles, and responsibilities of the security program, as well as the acceptable use, access control, incident response, and compliance requirements for the information assets. Assignment of roles and responsibilities: This is the process of identifying and assigning the specific tasks and duties related to the security program to the appropriate individuals or groups within the organization. Roles and responsibilities define who is accountable, responsible, consulted, and informed for each security activity, such as risk assessment, vulnerability management, threat detection, incident response, auditing, and reporting. Information asset classification: This is the process of categorizing the information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps to determine the appropriate level of protection and controls for each asset, as well as the impact and likelihood of a security breach or loss. Information asset classification also facilitates the prioritization of security resources and efforts based on the risk level of each asset.

QUESTION 5

The Chief Information Security Officer is directing a new program to reduce attack surface risks and threats as part of a zero trust approach. The IT security team is required to come up with priorities for the program. Which of the following is the best priority based on common attack frameworks?

A. Reduce the administrator and privileged access accounts

B. Employ a network-based IDS

C. Conduct thorough incident response

D. Enable SSO to enterprise applications

Correct Answer: A

The best priority based on common attack frameworks for a new program to reduce attack surface risks and threats as part of a zero trust approach is to reduce the administrator and privileged access accounts. Administrator and privileged access accounts are accounts that have elevated permissions or capabilities to perform sensitive or critical tasks on systems or networks, such as installing software, changing configurations, accessing data, or granting access. Reducing the administrator and privileged access accounts can help minimize the attack surface, as it can limit the number of potential targets or entry points for attackers, as well as reduce the impact or damage of an attack if an account is compromised.

QUESTION 6

A new prototype for a company\\'s flagship product was leaked on the internet. As a result, the management team has locked out all USB dives. Optical drive writers are not present on company computers. The sales team has been granted an exception to share sales presentation files with third parties. Which of the following would allow the IT team to determine which devices are USB enabled?

A. Asset tagging

B. Device encryption

C. Data loss prevention

D. SIEM logs

Correct Answer: D

QUESTION 7

A security analyst is monitoring a company\\'s network traffic and finds ping requests going to accounting and human resources servers from a SQL server. Upon investigation, the analyst discovers a technician responded to potential network connectivity issues. Which of the following is the best way for the security analyst to respond?

A. Report this activity as a false positive, as the activity is legitimate.

B. Isolate the system and begin a forensic investigation to determine what was compromised.

C. Recommend network segmentation to the management team as a way to secure the various environments.

D. Implement host-based firewalls on all systems to prevent ping sweeps in the future.

Correct Answer: A

Reporting this activity as a false positive, as the activity is legitimate, is the best way for the security analyst to respond. A false positive is a condition in which harmless traffic is classified as a potential network attack by a security monitoring tool. Ping requests are a common network diagnostic tool that can be used to test network connectivity issues. The technician who responded to potential network connectivity issues was performing a legitimate task and did not pose any threat to the accounting and human resources servers . https://www.techopedia.com/definition39/memory-dump

QUESTION 8

Which of the following best explains the importance of communicating with staff regarding the official public communication plan related to incidents impacting the organization?

A. To establish what information is allowed to be released by designated employees

B. To designate an external public relations firm to represent the organization

C. To ensure that all news media outlets are informed at the same time

D. To define how each employee will be contacted after an event occurs

Correct Answer: A

Communicating with staff about the official public communication plan is important to avoid unauthorized or inaccurate disclosure of information that could harm the organization\\'s reputation, security, or legal obligations. It also helps to ensure consistency and clarity of the messages delivered to the public and other stakeholders. https://resources.sei.cmu.edu/asset_files/Handbook/2021_002_001_651819.pdf

QUESTION 9

When investigating a potentially compromised host, an analyst observes that the process BGInfo.exe (PID 1024), a

Sysinternals tool used to create desktop backgrounds containing host details, has bee running for over two days. Which of the following activities will provide the best insight into this potentially malicious process, based on the anomalous behavior?

A. Changes to system environment variables

B. SMB network traffic related to the system process

C. Recent browser history of the primary user

D. Activities taken by PID 1024

Correct Answer: D

The activities taken by the process with PID 1024 will provide the best insight into this potentially malicious process, based on the anomalous behavior. BGInfo.exe is a legitimate tool that displays system information on the desktop background, but it can also be used by attackers to gather information about the compromised host or to disguise malicious processes12. By monitoring the activities of PID 1024, such as the files it accesses, the network connections it makes, or the commands it executes, the analyst can determine if the process is benign or malicious. References: bginfo.exe Windows process - What is it?, What is bginfo.exe? Is it Safe or a Virus? How to remove or fix it

QUESTION 10

A technician identifies a vulnerability on a server and applies a software patch. Which of the following should be the next step in the remediation process?

A. Testing

B. Implementation

C. Validation

D. Rollback

Correct Answer: C

The next step in the remediation process after applying a software patch is validation. Validation is a process that involves verifying that the patch has been successfully applied, that it has fixed the vulnerability, and that it has not caused any adverse effects on the system or application functionality or performance. Validation can be done using various methods, such as scanning, testing, monitoring, or auditing.

QUESTION 11

A security analyst has found a moderate-risk item in an organization\\'s point-of-sale application. The organization is currently in a change freeze window and has decided that the risk is not high enough to correct at this time. Which of the following inhibitors to remediation does this scenario illustrate?

A. Service-level agreement

B. Business process interruption

C. Degrading functionality

D. Proprietary system

Correct Answer: B

Business process interruption is the inhibitor to remediation that this scenario illustrates. Business process interruption is when the remediation of a vulnerability or an incident requires the disruption or suspension of a critical or essential business process, such as the point-of-sale application. This can cause operational, financial, or reputational losses for the organization, and may outweigh the benefits of the remediation. Therefore, the organization may decide to postpone or avoid the remediation until a more convenient time, such as a change freeze window, which is a period of time when no changes are allowed to the IT environment12. Service-level agreement, degrading functionality, and proprietary system are other possible inhibitors to remediation, but they are not relevant to this scenario. Service-level agreement is when the remediation of a vulnerability or an incident violates or affects the contractual obligations or expectations of the service provider or the customer. Degrading functionality is when the remediation of a vulnerability or an incident reduces or impairs the performance or usability of a system or an application. Proprietary system is when the remediation of a vulnerability or an incident involves a system or an application that is owned or controlled by a third party, and the organization has limited or no access or authority to modify it3. References: Inhibitors to Remediation -- SOC Ops Simplified, Remediation Inhibitors - CompTIA CySA+, Information security Vulnerability Management Report (Remediation...

QUESTION 12

A cybersecurity analyst is researching operational data to develop a script that will detect the presence of a threat on corporate assets. Which of the following contains the most useful information to produce this script?

A. API documentation

B. Protocol analysis captures

C. MITRE ATTandCK reports

D. OpenloC files

Correct Answer: C

A cybersecurity analyst is researching operational data to develop a script that will detect the presence of a threat on corporate assets. The most useful information to produce this script is MITRE ATTandCK reports. MITRE ATTandCK is a

knowledge base of adversary tactics and techniques based on real-world observations. MITRE ATTandCK reports provide detailed information on how different threat actors operate, what tools they use, what indicators they leave behind, and

how to detect or mitigate their attacks. The other options are not as useful or relevant for this purpose.

Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 9; https://attack.mitre.org/

QUESTION 13

An employee accessed a website that caused a device to become infected with invasive malware. The incident response analyst has:

1.

created the initial evidence log.

2.

disabled the wireless adapter on the device.

3.

interviewed the employee, who was unable to identify the website that was accessed.

4.

reviewed the web proxy traffic logs.

Which of the following should the analyst do to remediate the infected device?

A. Update the system firmware and reimage the hardware.

B. Install an additional malware scanner that will send email alerts to the analyst.

C. Configure the system to use a proxy server for Internet access.

D. Delete the user profile and restore data from backup.

Correct Answer: A

Updating the system firmware and reimaging the hardware is the best action to perform to remediate the infected device, as it helps to ensure that the device is restored to a clean and secure state and that any traces of malware are removed. Firmware is a type of software that controls the low-level functions of a hardware device, such as a motherboard, hard drive, or network card. Firmware can be updated or flashed to fix bugs, improve performance, or enhance security. Reimaging is a process of erasing and restoring the data on a storage device, such as a hard drive or a solid state drive, using an image file that contains a copy of the operating system, applications, settings, and files. Reimaging can help to recover from system failures, data corruption, or malware infections. Updating the system firmware and reimaging the hardware can help to remediate the infected device by removing any malicious code or configuration changes that may have been made by the malware, as well as restoring any missing or damaged files or settings that may have been affected by the malware. This can help to prevent further damage, data loss, or compromise of the device or the network. The other actions are not as effective or appropriate as updating the system firmware and reimaging the hardware, as they do not address the root cause of the infection or ensure that the device is fully cleaned and secured. Installing an additional malware scanner that will send email alerts to the analyst may help to detect and remove some types of malware, but it may not be able to catch all malware variants or remove them completely. It may also create conflicts or performance issues with other security tools or systems on the device. Configuring the system to use a proxy server for Internet access may help to filter or monitor some types of malicious traffic or requests, but it may not prevent or remove malware that has already infected the device or that uses other methods of communication or propagation. Deleting the user profile and restoring data from backup may help to recover some data or settings that may have been affected by the malware, but it may not remove malware that has infected other parts of the system or that has persisted on the device.

QUESTION 14

An organization would like to ensure its cloud infrastructure has a hardened configuration. A requirement is to create a server image that can be deployed with a secure template. Which of the following is the best resource to ensure secure configuration?

A. CIS Benchmarks

B. PCI DSS

C. OWASP Top Ten

D. ISO 27001

Correct Answer: A

The best resource to ensure secure configuration of cloud infrastructure is A. CIS Benchmarks. CIS Benchmarks are a set of prescriptive configuration recommendations for various technologies, including cloud providers, operating systems, network devices, and server software. They are developed by a global community of cybersecurity experts and help organizations protect their systems against threats more confidently1 PCI DSS, OWASP Top Ten, and ISO 27001 are also important standards for information security, but they are not focused on providing specific guidance for hardening cloud infrastructure. PCI DSS is a compliance scheme for payment card transactions, OWASP Top Ten is a list of common web application security risks, and ISO 27001 is a framework for establishing and maintaining an information security management system. These standards may have some relevance for cloud security, but they are not as comprehensive and detailed as CIS Benchmarks

QUESTION 15

A security team is concerned about recent Layer 4 DDoS attacks against the company website. Which of the following controls would best mitigate the attacks?

A. Block the attacks using firewall rules.

B. Deploy an IPS in the perimeter network.

C. Roll out a CDN.

D. Implement a load balancer.

Correct Answer: C

Rolling out a CDN is the best control to mitigate the Layer 4 DDoS attacks against the company website. A CDN is a Content Delivery Network, which is a system of distributed servers that deliver web content to users based on their geographic location, the origin of the web page, and the content delivery server. A CDN can help protect against Layer 4 DDoS attacks, which are volumetric attacks that aim to exhaust the network bandwidth or resources of the target website by sending a large amount of traffic, such as SYN floods, UDP floods, or ICMP floods. A CDN can mitigate these attacks by distributing the traffic across multiple servers, caching the web content closer to the users, filtering out malicious or unwanted traffic, and providing scalability and redundancy for the website12. References: How to Stop a DDoS Attack: Mitigation Steps for Each OSI Layer, Application layer DDoS attack | Cloudflare