CAS-005 Q&As

CompTIA SecurityX Exam

Pass CompTIA CAS-005 Exam with 100% Guarantee

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

https://www.leads4pass.com/cas-005.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An IT director is working on a solution to meet the challenge of remotely managing laptop devices and securely locking them down. The solution must meet the following requirements:

1.

Cut down on patch management.

2.

Make use of standard configurations.

3.

Allow for custom resource configurations.

4.

Provide access to the enterprise system from multiple types of devices.

Which of the following would meet these requirements?

A. MDM

B. Emulator

C. Hosted hypervisor

D. VDI

Correct Answer: D

Cut down on patch management: With VDI, the virtual desktops are managed centrally. Patches and updates can be applied to the master image, which then gets propagated to all virtual desktops. This significantly reduces the complexity and workload of patch management. Standard configurations: VDI allows for the deployment of standardized desktop images, ensuring consistency across all user desktops. Allow for custom resource configurations: VDI can be configured to allocate different levels of resources (CPU, memory, storage) based on the needs of different users or groups. Provide access to the enterprise system from multiple types of devices: Users can access their virtual desktops from various devices, including laptops, tablets, and smartphones, as long as they have a network connection.

QUESTION 2

A company updates its cloud-based services by saving infrastructure code in a remote repository. The code is automatically deployed into the development environment every time the code is saved lo the repository The developers express concern that the deployment often fails, citing minor code issues and occasional security control check failures in the development environment

Which of the following should a security engineer recommend to reduce the deployment failures? (Select two).

A. Software composition analysis

B. Pre-commit code linting

C. Repository branch protection

D. Automated regression testing

E. Code submit authorization workflow

F. Pipeline compliance scanning

Correct Answer: BD

B. Pre-commit code linting: Linting tools analyze code for syntax errors and adherence to coding standards before the code is committed to the repository. This helps catch minor code issues early in the development process, reducing the

likelihood of deployment failures.

D. Automated regression testing: Automated regression tests ensure that new code changes do not introduce bugs or regressions into the existing codebase. By running these tests automatically during the deployment process, developers

can catch issues early and ensure the stability of the development environment.

Other options:

A. Software composition analysis: This helps identify vulnerabilities in third-party components but does not directly address code quality or deployment failures. C. Repository branch protection: While this can help manage the code

submission process, it does not directly prevent deployment failures caused by code issues or security check failures.

E. Code submit authorization workflow: This manages who can submit code but does not address the quality of the code being submitted. F. Pipeline compliance scanning: This checks for compliance with security policies but does not

address syntax or regression issues.

References:

CompTIA Security+ Study Guide

"Continuous Integration and Continuous Delivery" by Jez Humble and David Farley

OWASP (Open Web Application Security Project) guidelines on secure coding practices

QUESTION 3

A compliance officer is responsible for selecting the right governance framework to protect individuals\\' data. Which of the following is the appropriate framework for the company to consult when collecting international user data for the

purpose of processing credit cards?

A. ISO 27001

B. COPPA

C. NIST 800-53

D. PCI DSS

Correct Answer: D

QUESTION 4

A company receives several complaints from customers regarding its website. An engineer implements a parser for the web server logs that generates the following output:

Browser	User location	Load time	HTTP response
Mozilla 5.0	United States	190ms	302
Chrome 110	France	1.2s	302
Microsoft Edge	India	3.7s	307
Microsoft Edge	Australia	6.4s	200

which of the following should the company implement to best resolve the issue?

A. IDS

B. CDN

C. WAF

D. NAC

Correct Answer: B

The table indicates varying load times for users accessing the website from different geographic locations. Customers from Australia and India are experiencing significantly higher load times compared to those from the United States. This suggests that latency and geographical distance are affecting the website\\'s performance. A. IDS (Intrusion Detection System): While an IDS is useful for detecting malicious activities, it does not address performance issues related to latency and geographical distribution of content.

B. CDN (Content Delivery Network): A CDN stores copies of the website\\'s content in multiple geographic locations. By serving content from the nearest server to the user, a CDN can significantly reduce load times and improve user

experience globally.

C. WAF (Web Application Firewall): A WAF protects web applications by filtering and monitoring HTTP traffic but does not improve performance related to geographical latency. D. NAC (Network Access Control): NAC solutions control access

to network resources but are not designed to address web performance issues. Implementing a CDN is the best solution to resolve the performance issues observed in the log output.

References:

CompTIA Security+ Study Guide

"CDN: Content Delivery Networks Explained" by Akamai Technologies NIST SP 800-44, "Guidelines on Securing Public Web Servers"

QUESTION 5

An organization wants to manage specialized endpoints and needs a solution that provides the ability to:

1.

Centrally manage configurations

2.

Push policies.

3.

Remotely wipe devices

4.

Maintain asset inventory

Which of the following should the organization do to best meet these requirements?

A. Use a configuration management database

B. Implement a mobile device management solution.

C. Configure contextual policy management

D. Deploy a software asset manager

Correct Answer: B

To meet the requirements of centrally managing configurations, pushing policies, remotely wiping devices, and maintaining an asset inventory, the best solution is to implement a Mobile Device Management (MDM) solution.

MDM Capabilities:

Central Management: MDM allows administrators to manage the configurations of all devices from a central console.

Policy Enforcement: MDM solutions enable the push of security policies and updates to ensure compliance across all managed devices. Remote Wipe: In case a device is lost or stolen, MDM provides the capability to remotely wipe the device

to protect sensitive data. Asset Inventory: MDM maintains an up-to-date inventory of all managed devices, including their configurations and installed applications. Other options do not provide the same comprehensive capabilities required for

managing specialized endpoints.

References:

CompTIA SecurityX Study Guide

NIST Special Publication 800-124 Revision 1, "Guidelines for Managing the Security of Mobile Devices in the Enterprise"

"Mobile Device Management Overview," Gartner Research

QUESTION 6

A security analyst discovered requests associated with IP addresses known for born legitimate 3nd bot-related traffic.

Which of the following should the analyst use to determine whether the requests are malicious?

A. User-agent string

B. Byte length of the request

C. Web application headers

D. HTML encoding field

Correct Answer: A

The user-agent string can provide valuable information to distinguish between legitimate and bot-related traffic. It contains details about the browser, device, and sometimes the operating system of the client making the request.

Why Use User-Agent String?

Identify Patterns: User-agent strings can help identify patterns that are typical of bots or legitimate users.

Block Malicious Bots: Many bots use known user-agent strings, and identifying these can help block malicious requests.

Anomalies Detection: Anomalous user-agent strings can indicate spoofing attempts or malicious activity.

Other options provide useful information but may not be as effective for initial determination of the nature of the request:

B. Byte length of the request: This can indicate anomalies but does not provide detailed information about the client.

C. Web application headers: While useful, they may not provide enough distinction between legitimate and bot traffic.

D. HTML encoding field: This is not typically used for identifying the nature of the request.

References:

CompTIA SecurityX Study Guide

"User-Agent Analysis for Security," OWASP

NIST Special Publication 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)"

QUESTION 7

A security operations engineer needs to prevent inadvertent data disclosure when encrypted SSDs are reused within an enterprise.

Which of the following is the most secure way to achieve this goal?

A. Executing a script that deletes and overwrites all data on the SSD three times

B. Wiping the SSD through degaussing

C. Securely deleting the encryption keys used by the SSD

D. Writing non-zero, random data to all cells of the SSD

Correct Answer: C

The most secure way to prevent inadvertent data disclosure when encrypted SSDs are reused is to securely delete the encryption keys used by the SSD. Without the encryption keys, the data on the SSD remains encrypted and is effectively

unreadable, rendering any residual data useless. This method is more reliable and efficient than overwriting data multiple times or using other physical destruction methods.

References:

CompTIA SecurityX Study Guide: Highlights the importance of managing encryption keys and securely deleting them to protect data. NIST Special Publication 800-88, "Guidelines for Media Sanitization":

Recommends cryptographic erasure as a secure method for sanitizing encrypted storage devices.

QUESTION 8

A security architect for a global organization with a distributed workforce recently received funding lo deploy a CASB solution

Which of the following most likely explains the choice to use a proxy-based CASB?

A. The capability to block unapproved applications and services is possible

B. Privacy compliance obligations are bypassed when using a user-based deployment.

C. Protecting and regularly rotating API secret keys requires a significant time commitment

D. Corporate devices cannot receive certificates when not connected to on-premises devices

Correct Answer: A

A proxy-based Cloud Access Security Broker (CASB) is chosen primarily for its ability to block unapproved applications and services. Here\\'s why:

Application and Service Control: Proxy-based CASBs can monitor and control the use of applications and services by inspecting traffic as it passes through the proxy. This allows the organization to enforce policies that block unapproved

applications and services, ensuring compliance with security policies. Visibility and Monitoring: By routing traffic through the proxy, the CASB can provide detailed visibility into user activities and data flows, enabling better monitoring and

threat detection.

Real-Time Protection: Proxy-based CASBs can provide real-time protection against threats by analyzing and controlling

traffic before it reaches the end user, thus preventing the use of risky applications and services.

QUESTION 9

A junior security researcher has identified a buffer overflow vulnerability leading to remote code execution in a former employer\\'s software. The security researcher asks for the manager\\'s advice on the vulnerability submission process. Which of the following is the best advice the current manager can provide the security researcher?

A. Collect proof that the exploit works in order to expedite the process.

B. Publish proof-of-concept exploit code on a personal blog.

C. Recommend legal consultation about the process.

D. Visit a bug bounty website for the latest information.

Correct Answer: C

Legal consultation is crucial before proceeding with any vulnerability disclosure process, especially when dealing with vulnerabilities found in former employers\\' software. It ensures that the researcher adheres to legal and ethical standards, protects their rights, and avoids potential legal risks associated with disclosure. Therefore, advising the security researcher to seek legal consultation is the most prudent course of action in this situation.

QUESTION 10

SIMULATION

As a security administrator, you are asked to harden a server running Red Hat Enterprise Server 5.5 64-bit.

This server is being used as a DNS and time server. It is not used as a database, web server, or print server. There are no wireless connections to the server, and it does not need to print.

The command window will be provided along with root access. You are connected via a secure shell with root access.

You may query help for a list of commands.

Instructions:

You need to disable and turn off unrelated services and processes.

It is possible to simulate a crash of your server session. The simulation can be reset, but the server cannot be rebooted. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

A. See the complete solution below in Explanation.

B. PlaceHoder

C. PlaceHoder

D. PlaceHoder

Correct Answer: A

In Order to deactivate web services, database services and print service, we can do following things 1) deactivate its services /etc/init.d/apache2 stop /etc/init.d/mysqld stop 2) close ports for these services Web Server iptables -I INPUT -p tcp -m tcp --dport 443 -j REJECTservice iptables save Print Server iptables -I INPUT -p tcp -m tcp --dport 631 -j REJECTservice iptables save Database Server iptables -I INPUT -p tcp -m tcp --dport -j REJECTservice iptables save 3) Kill the process any running for the same ps -aef|grep mysql kill -9

QUESTION 11

A company recently experienced an incident in which an advanced threat actor was able to shim malicious code against the hardware static of a domain controller The forensic team cryptographically validated that com the underlying firmware of the box and the operating system had not been compromised. However, the attacker was able to exfiltrate information from the server using a steganographic technique within LOAP

Which of the following is me best way to reduce the risk oi reoccurrence?

A. Enforcing allow lists for authorized network pons and protocols

B. Measuring and attesting to the entire boot chum

C. Rolling the cryptographic keys used for hardware security modules

D. Using code signing to verify the source of OS updates

Correct Answer: A

The scenario describes a sophisticated attack where the threat actor used steganography within LDAP to exfiltrate data. Given that the hardware and OS firmware were validated and found uncompromised, the attack vector likely exploited a

network communication channel. To mitigate such risks, enforcing allow lists for authorized network ports and protocols is the most effective strategy.

Here\\'s why this option is optimal:

Port and Protocol Restrictions: By creating an allow list, the organization can restrict communications to only those ports and protocols that are necessary for legitimate business operations. This reduces the attack surface by preventing

unauthorized or unusual traffic.

Network Segmentation: Enforcing such rules helps in segmenting the network and ensuring that only approved communications occur, which is critical in preventing data exfiltration methods like steganography. Preventing Unauthorized

Access: Allow lists ensure that only predefined, trusted connections are allowed, blocking potential paths that attackers could use to infiltrate or exfiltrate data.

Other options, while beneficial in different contexts, are not directly addressing the network communication threat:

B. Measuring and attesting to the entire boot chain: While this improves system integrity, it doesn\\'t directly mitigate the risk of data exfiltration through network channels. C. Rolling the cryptographic keys used for hardware security modules:

This is useful for securing data and communications but doesn\\'t directly address the specific method of exfiltration described. D. Using code signing to verify the source of OS updates: Ensures updates are from legitimate sources, but it

doesn\\'t mitigate the risk of network-based data exfiltration.

References:

CompTIA SecurityX Study Guide

NIST Special Publication 800-41, "Guidelines on Firewalls and Firewall Policy" CIS Controls Version 8, Control 9: Limitation and Control of Network Ports, Protocols, and Services

QUESTION 12

A hospital provides tablets to its medical staff to enable them to more quickly access and edit patients\\' charts. The hospital wants to ensure that if a tablet is Identified as lost or stolen and a remote command is issued, the risk of data loss can be mitigated within seconds. The tablets are configured as follows to meet hospital policy

1.

Full disk encryption is enabled

2.

Always O"; corporate VPN is enabled

3.

ef-use-backed keystore is enabled\\'ready.

4.

Wi-Fi 6 is configured with SAE.

5.

Location services is disabled.

6.

Application allow list is configured

A. Revoking the user certificates used for VPN and Wi-Fi access

B. Performing cryptographic obfuscation

C. Using geolocation to find the device

D. Configuring the application allow list to only per mil emergency calls

E. Returning on the device\\'s solid-state media to zero

Correct Answer: E

To mitigate the risk of data loss on a lost or stolen tablet quickly, the most effective strategy is to return the device\\'s solid-state media to zero, which effectively erases all data on the device. Here\\'s why:

Immediate Data Erasure: Returning the solid-state media to zero ensures that all data is wiped instantly, mitigating the risk of data loss if the device is lost or stolen. Full Disk Encryption: Even though the tablets are already encrypted,

physically erasing the data ensures that no residual data can be accessed if someone attempts to bypass encryption.

Compliance and Security: This method adheres to best practices for data security and compliance, ensuring that sensitive patient data cannot be accessed by unauthorized parties.

QUESTION 13

An organization needs to classify its systems and data in accordance with external requirements. Which of the following roles is best qualified to perform this task?

A. Systems administrator

B. Data owner

C. Data processor

D. Data custodian

E. Data steward

Correct Answer: B

QUESTION 14

A company uses a CSP to provide a front end for its new payment system offering. The new offering is currently certified as PCI compliant. In order for the integrated solution to be compliant, the customer:

A. must also be PCI compliant, because the risk is transferred to the provider.

B. still needs to perform its own PCI assessment of the provider\\'s managed serverless service.

C. needs to perform a penetration test of the cloud provider\\'s environment.

D. must ensure in-scope systems for the new offering are also PCI compliant.

Correct Answer: D

QUESTION 15

A common industrial protocol has the following characteristics:

1.

Provides for no authentication/security

2.

Is often implemented in a client/server relationship

3.

Is implemented as either RTU or TCP/IP

Which of the following is being described?

A. Profinet

B. Modbus

C. Zigbee

D. Z-Wave

Correct Answer: B