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

Which of the following best explains the importance of determining organization risk appetite when operating with a constrained budget?

A. Risk appetite directly impacts acceptance of high-impact low-likelihood events.

B. Organizational risk appetite varies from organization to organization

C. Budgetary pressure drives risk mitigation planning in all companies

D. Risk appetite directly influences which breaches are disclosed publicly

Correct Answer: A

Risk appetite is the amount of risk an organization is willing to accept to achieve its objectives. When operating with a constrained budget, understanding the organization\\'s risk appetite is crucial because:

It helps prioritize security investments based on the level of risk the organization is willing to tolerate.

High-impact, low-likelihood events may be deemed acceptable if they fall within the organization\\'s risk appetite, allowing for budget allocation to other critical areas. Properly understanding and defining risk appetite ensures that limited

resources are used effectively to manage risks that align with the organization\\'s strategic goals.

References:

CompTIA Security+ Study Guide

NIST Risk Management Framework (RMF) guidelines

ISO 31000, "Risk Management ?Guideline";

QUESTION 2

IoCs were missed during a recent security incident due to the reliance on a signature-based detection platform. A security engineer must recommend a solution that can be implemented to address this shortcoming. Which of the following would be the most appropriate recommendation?

A. FIM

B. SASE

C. UEBA

D. CSPM

E. EAP

Correct Answer: C

UEBA focuses on analyzing the behaviors of users and entities within the network to identify anomalies that may

indicate security threats. Unlike signature-based detection, which relies on known patterns of malicious activity, UEBA uses machine learning and advanced analytics to detect deviations from normal behavior. This approach can identify new and unknown threats that do not match existing signatures, thus addressing the limitation of missing IoCs that signature-based systems might overlook

QUESTION 3

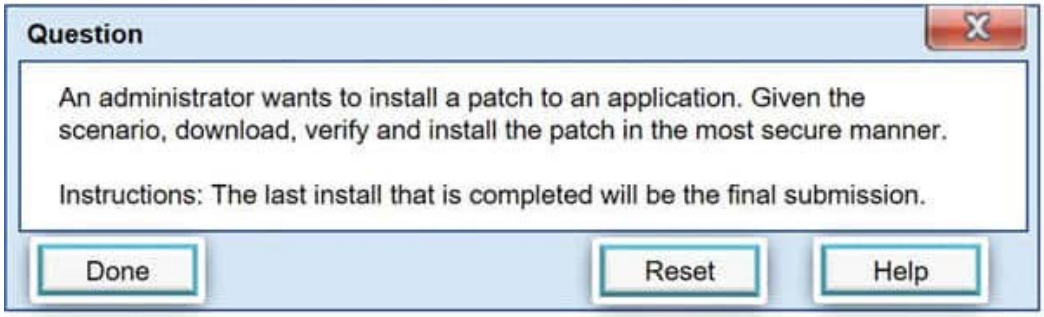
SIMULATION

HOME>Download Center>Application Patch

The links in this section correspond to separate files available in this download center. Download the most appropriate file.

File Name	Mirror	Download Files Below
Install.exe	Mirror 1	Download
Install.exe	Mirror 2	Download
Install.exe	Mirror 3	Download
Install.exe	Mirror 4	Download
Install.exe	Mirror 5	Download
Install.exe	Mirror 6	Download

HASH: 1759adb5g34700aae19bc4578fc19cc2



A. See the complete solution below in Explanation.

B. PlaceHoder

C. PlaceHoder

D. PlaceHoder

Correct Answer: A

Step 1: Verify that the certificate is valid or not. In case of any warning message, cancel the download.

Step 2: If certificate issue is not there then, download the file in your system.

Step 3: Calculate the hash value of the downloaded file.

Step 4: Match the hash value of the downloaded file with the one which you selected on the website. Step 5: Install the file if the hash value matches.

QUESTION 4

An internal security audit determines that Telnet is currently being used within the environment to manage network switches. Which of the following tools should be utilized to identify credentials in plaintext that are used to log in to these devices?

A. Fuzzer

B. Network traffic analyzer

C. HTTP interceptor

D. Port scanner

E. Password cracker

Correct Answer: B

A network traffic analyzer (also known as a packet sniffer or protocol analyzer) captures and inspects the data packets traveling over the network. Since Telnet transmits data, including credentials, in plaintext, a network traffic analyzer can be used to capture the packets containing the login credentials as they are sent over the network. Tools like Wireshark are commonly used for this purpose and can help identify and analyze the plaintext credentials.

QUESTION 5

A company hosts a platform-as-a-service solution with a web-based front end, through which customer interact with data sets. A security administrator needs to deploy controls to prevent application-focused attacks.

Which of the following most directly supports the administrator\\'s objective\\'

A. improving security dashboard visualization on SIEM

B. Rotating API access and authorization keys every two months

C. Implementing application toad balancing and cross-region availability

D. Creating WAF policies for relevant programming languages

Correct Answer: D

The best way to prevent application-focused attacks for a platform-as-a- service solution with a web-based front end is to create Web Application Firewall (WAF) policies for relevant programming languages. Here\\'s why:

Application-Focused Attack Prevention: WAFs are designed to protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. They help prevent attacks such as SQL injection, cross-site scripting

(XSS), and other application-layer attacks.

Customizable Rules: WAF policies can be tailored to the specific programming languages and frameworks used by the web application, providing targeted protection based on known vulnerabilities and attack patterns. Real-Time Protection:

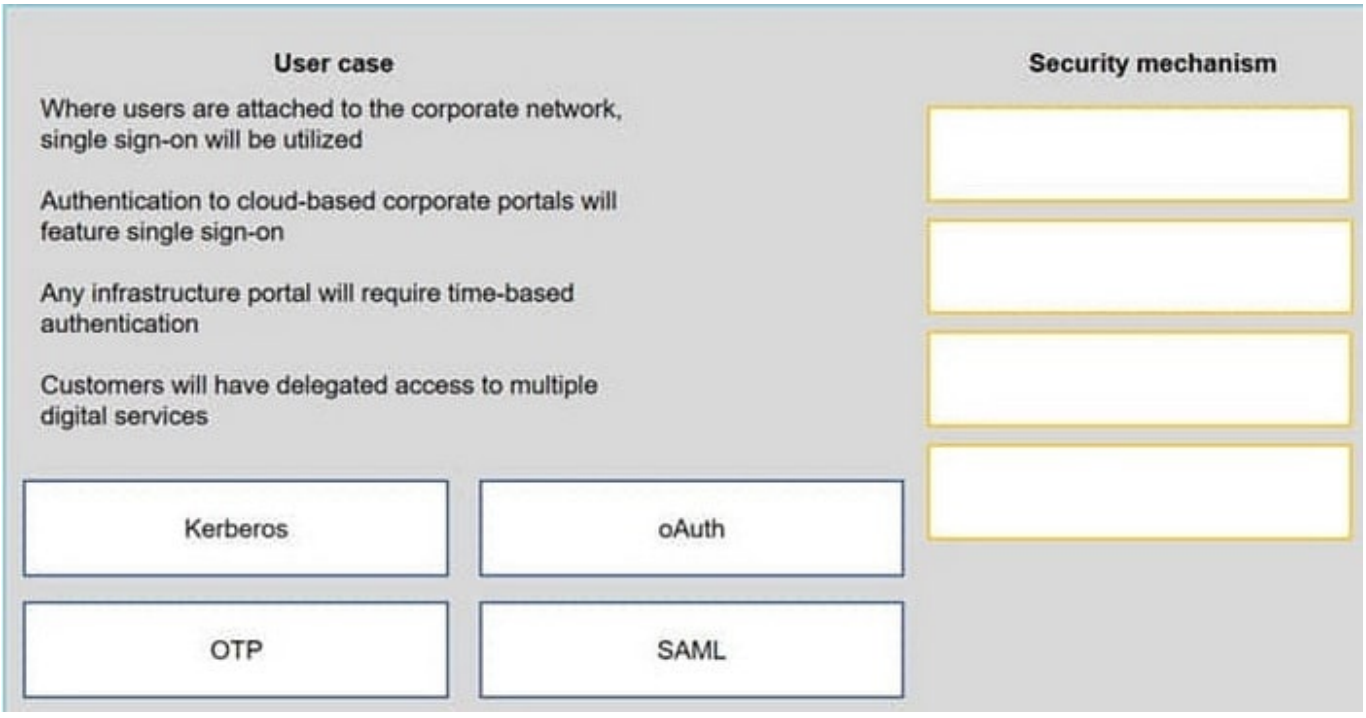
WAFs provide real-time protection, blocking malicious requests before they reach the application, thereby enhancing the security posture of the platform.

QUESTION 6

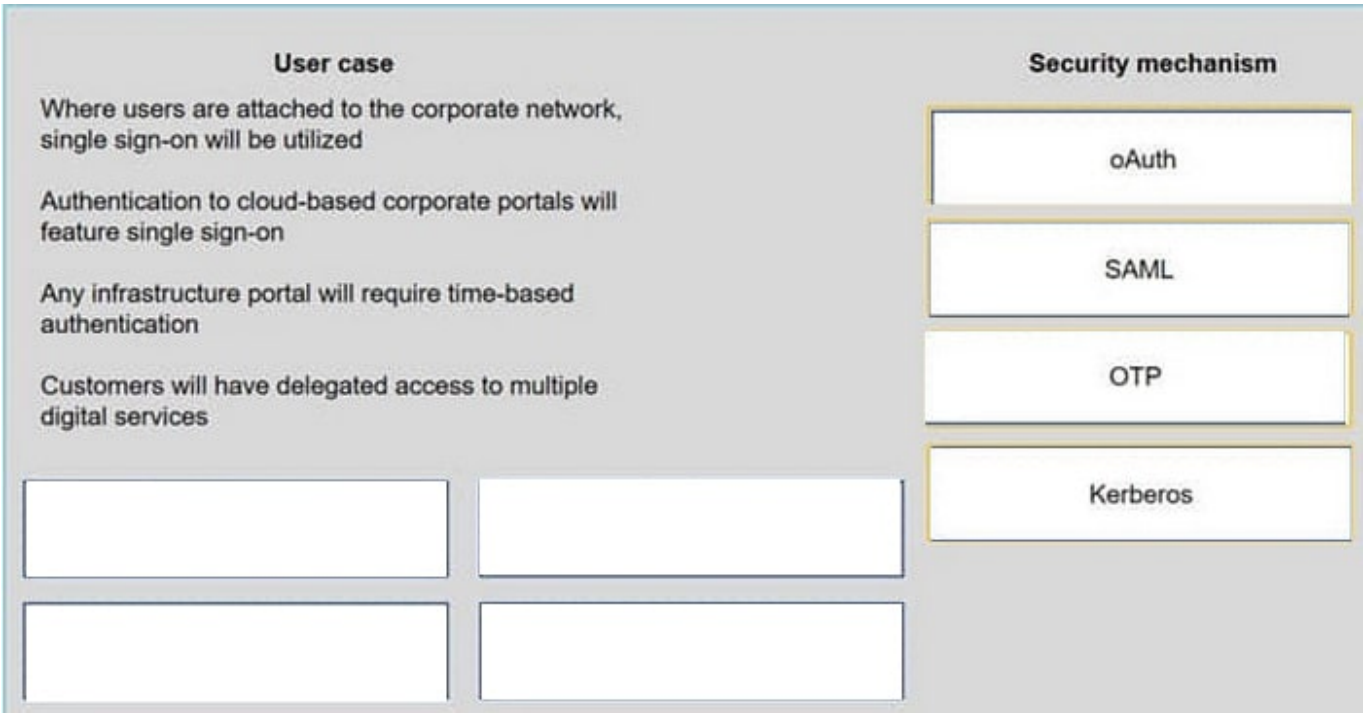
DRAG DROP

A security consultant is considering authentication options for a financial institution. The following authentication options are available security mechanism to the appropriate use case. Options may be used once.

Select and Place:



Correct Answer:



QUESTION 7

Developers have been creating and managing cryptographic material on their personal laptops fix use in production environment. A security engineer needs to initiate a more secure process.

Which of the following is the best strategy for the engineer to use?

A. Disabling the BIOS and moving to UEFI

B. Managing secrets on the vTPM hardware

C. Employing shielding lo prevent LMI

D. Managing key material on a HSM

Correct Answer: D

The best strategy for securely managing cryptographic material is to use a Hardware Security Module (HSM). Here\\'s why:

Security and Integrity: HSMs are specialized hardware devices designed to protect and manage digital keys. They provide high levels of physical and logical security, ensuring that cryptographic material is well protected against tampering

and unauthorized access.

Centralized Key Management: Using HSMs allows for centralized management of cryptographic keys, reducing the risks associated with decentralized and potentially insecure key storage practices, such as on personal laptops. Compliance

and Best Practices: HSMs comply with various industry standards and regulations (such as FIPS 140-2) for secure key management. This ensures that the organization adheres to best practices and meets compliance requirements.

QUESTION 8

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 9

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 10

To bring digital evidence in a court of law, the evidence must be:

A. material.

B. tangible.

C. consistent.

D. conserved.

Correct Answer: A

For evidence to be admissible in court, it must be material, meaning it must be relevant and have a significant impact on the case. Material evidence directly relates to the facts in dispute and can affect the outcome of the case by proving or disproving a key point.

QUESTION 11

A cybersecurity architect is reviewing the detection and monitoring capabilities for a global company that recently made multiple acquisitions.

The architect discovers that the acquired companies use different vendors for detection and monitoring

The architect\\'s goal is to:

1.

Create a collection of use cases to help detect known threats

2.

Include those use cases in a centralized library for use across all of the companies

Which of the following is the best way to achieve this goal?

A. Sigma rules

B. Ariel Query Language

C. UBA rules and use cases

D. TAXII/STIX library

Correct Answer: A

To create a collection of use cases for detecting known threats and include them in a centralized library for use across multiple companies with different vendors, Sigma rules are the best option. Here\\'s why: Vendor-Agnostic Format: Sigma rules are a generic and open standard for writing SIEM (Security Information and Event Management) rules. They can be translated to specific query languages of different SIEM systems, making them highly versatile and applicable across various platforms. Centralized Rule Management: By using Sigma rules, the cybersecurity architect can create a centralized library of detection rules that can be easily shared and implemented across different detection and monitoring systems used by the acquired companies. This ensures consistency in threat detection capabilities. Ease of Use and Flexibility: Sigma provides a structured and straightforward format for defining detection logic. It allows for the easy creation, modification, and sharing of rules, facilitating collaboration and standardization across the organization.

QUESTION 12

An organization is looking for gaps in its detection capabilities based on the APTs that may target the industry

Which of the following should the security analyst use to perform threat modeling?

A. ATTandCK

B. OWASP

C. CAPEC

D. STRIDE

Correct Answer: A

The ATTandCK (Adversarial Tactics, Techniques, and Common Knowledge) framework is the best tool for a security analyst to use for threat modeling when looking for gaps in detection capabilities based on Advanced Persistent Threats

(APTs) that may target the industry. Here\\'s why:

Comprehensive Framework: ATTandCK provides a detailed and structured repository of known adversary tactics and techniques based on real-world observations. It helps organizations understand how attackers operate and what techniques

they might use.

Gap Analysis: By mapping existing security controls against the ATTandCK matrix, analysts can identify which tactics and techniques are not adequately covered by current detection and mitigation measures. Industry Relevance: The ATTandCK

framework is continuously updated with the latest threat intelligence, making it highly relevant for industries facing APT threats. It provides insights into specific APT groups and their preferred methods of attack.

QUESTION 13

Recently, two large engineering companies in the same line of business decided to approach cyberthreats in a united way. Which of the following best describes this unified approach?

A. NDA

B. ISA

C. SLA

D. MOU

Correct Answer: D

Given the scenario of two large engineering companies joining forces to address cyberthreats in a united way, the most fitting description of their approach is a Memorandum of Understanding (MOU). This document formalizes their agreement to cooperate on cybersecurity matters, outlining their shared objectives, responsibilities, and possibly the methods they will use to collaborate effectively in combating cyber threats.

QUESTION 14

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 15

A security analyst is reviewing suspicious emails that were forwarded by users. Which of the following is the best method for the analyst to use when reviewing attachments that came with these emails?

A. Reverse engineering

B. Protocol analysis

C. Sandboxing

D. Fuzz testing

E. Steganography

Correct Answer: C

The most effective method for a security analyst to review suspicious email attachments is to use sandboxing. This approach allows the attachments to be executed in a safe, isolated environment, making it possible to observe any malicious activities without risking the integrity of the actual systems. Sandboxing offers a comprehensive and efficient way to analyze potentially harmful content in email attachments.

Latest CAS-005 Dumps CAS-005 Study Guide CAS-005 Exam Questions