

## Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

<https://www.2passeasy.com/dumps/CAS-004/>



#### NEW QUESTION 1

A disaster recovery team learned of several mistakes that were made during the last disaster recovery parallel test. Computational resources ran out at 70% of restoration of critical services.

Which of the following should be modified to prevent the issue from reoccurring?

- A. Recovery point objective
- B. Recovery time objective
- C. Mission-essential functions
- D. Recovery service level

**Answer:** B

#### Explanation:

Reference: <https://www.nakivo.com/blog/disaster-recovery-in-cloud-computing/>

#### NEW QUESTION 2

A company processes data subject to NDAs with partners that define the processing and storage constraints for the covered data. The agreements currently do not permit moving the covered data to the cloud, and the company would like to renegotiate the terms of the agreements.

Which of the following would MOST likely help the company gain consensus to move the data to the cloud?

- A. Designing data protection schemes to mitigate the risk of loss due to multitenancy
- B. Implementing redundant stores and services across diverse CSPs for high availability
- C. Emulating OS and hardware architectures to blur operations from CSP view
- D. Purchasing managed FIM services to alert on detected modifications to covered data

**Answer:** A

#### NEW QUESTION 3

An IT administrator is reviewing all the servers in an organization and notices that a server is missing crucial practice against a recent exploit that could gain root access.

Which of the following describes the administrator's discovery?

- A. A vulnerability
- B. A threat
- C. A breach
- D. A risk

**Answer:** A

#### Explanation:

Reference: <https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained>

#### NEW QUESTION 4

A high-severity vulnerability was found on a web application and introduced to the enterprise. The vulnerability could allow an unauthorized user to utilize an open-source library to view privileged user information. The enterprise is unwilling to accept the risk, but the developers cannot fix the issue right away. Which of the following should be implemented to reduce the risk to an acceptable level until the issue can be fixed?

- A. Scan the code with a static code analyzer, change privileged user passwords, and provide security training.
- B. Change privileged usernames, review the OS logs, and deploy hardware tokens.
- C. Implement MFA, review the application logs, and deploy a WAF.
- D. Deploy a VPN, configure an official open-source library repository, and perform a full application review for vulnerabilities.

**Answer:** D

**Explanation:**

Reference: <https://www.microfocus.com/en-us/what-is/sast>

**NEW QUESTION 5**

In preparation for the holiday season, a company redesigned the system that manages retail sales and moved it to a cloud service provider. The new infrastructure did not meet the company's availability requirements. During a postmortem analysis, the following issues were highlighted:

- \* 1. International users reported latency when images on the web page were initially loading.
- \* 2. During times of report processing, users reported issues with inventory when attempting to place orders.
- \* 3. Despite the fact that ten new API servers were added, the load across servers was heavy at peak times.

Which of the following infrastructure design changes would be BEST for the organization to implement to avoid these issues in the future?

- A. Serve static content via distributed CDNs, create a read replica of the central database and pull reports from there, and auto-scale API servers based on performance.
- B. Increase the bandwidth for the server that delivers images, use a CDN, change the database to a non-relational database, and split the ten API servers across two load balancers.
- C. Serve images from an object storage bucket with infrequent read times, replicate the database across different regions, and dynamically create API servers based on load.
- D. Serve static-content object storage across different regions, increase the instance size on the managed relational database, and distribute the ten API servers across multiple regions.

**Answer:** A

**NEW QUESTION 6**

A company has decided to purchase a license for software that is used to operate a mission-critical process. The third-party developer is new to the industry but is delivering what the company needs at this time.

Which of the following BEST describes the reason why utilizing a source code escrow will reduce the operational risk to the company if the third party stops supporting the application?

- A. The company will have access to the latest version to continue development.
- B. The company will be able to force the third-party developer to continue support.
- C. The company will be able to manage the third-party developer's development process.
- D. The company will be paid by the third-party developer to hire a new development team.

**Answer:** B

**NEW QUESTION 7**

A security engineer estimates the company's popular web application experiences 100 attempted breaches per day. In the past four years, the company's data has been breached two times.

Which of the following should the engineer report as the ARO for successful breaches?

- A. 0.5
- B. 8
- C. 50
- D. 36,500

**Answer:** A

**Explanation:**

Reference: <https://blog.netwrix.com/2020/07/24/annual-loss-expectancy-and-quantitative-risk-analysis/>

**NEW QUESTION 8**

During a system penetration test, a security engineer successfully gained access to a shell on a Linux host as a standard user and wants to elevate the privilege levels.

Which of the following is a valid Linux post-exploitation method to use to accomplish this goal?

- A. Spawn a shell using sudo and an escape string such as `sudo vim -c '!sh'`.
- B. Perform ASIC password cracking on the host.
- C. Read the `/etc/passwd` file to extract the usernames.
- D. Initiate unquoted service path exploits.
- E. Use the UNION operator to extract the database schema.

**Answer:** C

**Explanation:**

Reference: <https://docs.rapid7.com/insightvm/elevating-permissions/>

**NEW QUESTION 9**

An e-commerce company is running a web server on premises, and the resource utilization is usually less than 30%. During the last two holiday seasons, the server experienced performance issues because of too many connections, and several customers were not able to finalize purchase orders. The company is looking to change the server configuration to avoid this kind of performance issue.

Which of the following is the MOST cost-effective solution?

- A. Move the server to a cloud provider.
- B. Change the operating system.
- C. Buy a new server and create an active-active cluster.
- D. Upgrade the server with a new one.

**Answer:** A

**NEW QUESTION 10**

Device event logs sources from MDM software as follows:

Which of the following security concerns and response actions would BEST address the risks posed by the device in the logs?

- A. Malicious installation of an application; change the MDM configuration to remove application ID 1220.
- B. Resource leak; recover the device for analysis and clean up the local storage.
- C. Impossible travel; disable the device's account and access while investigating.
- D. Falsified status reporting; remotely wipe the device.

**Answer:** A

**NEW QUESTION 10**

A home automation company just purchased and installed tools for its SOC to enable incident identification and response on software the company develops. The company would like to prioritize defenses against the following attack scenarios:

Unauthorized insertions into application development environments

Authorized insiders making unauthorized changes to environment configurations Which of the following actions will enable the data feeds needed to detect these types of attacks on development environments? (Choose two.)

- A. Perform static code analysis of committed code and generate summary reports.
- B. Implement an XML gateway and monitor for policy violations.
- C. Monitor dependency management tools and report on susceptible third-party libraries.
- D. Install an IDS on the development subnet and passively monitor for vulnerable services.
- E. Model user behavior and monitor for deviations from normal.
- F. Continuously monitor code commits to repositories and generate summary logs.

**Answer:** CD

**NEW QUESTION 15**

Which of the following terms refers to the delivery of encryption keys to a CASB or a third-party entity?

- A. Key sharing
- B. Key distribution
- C. Key recovery
- D. Key escrow

**Answer:** B

**Explanation:**

Reference: <https://www.open.edu/openlearn/ocw/mod/oucontent/view.php?id=48322&ion=1.3>

#### NEW QUESTION 16

A company hired a third party to develop software as part of its strategy to be quicker to market. The company's policy outlines the following requirements: The credentials used to publish production software to the container registry should be stored in a secure location. Access should be restricted to the pipeline service account, without the ability for the third-party developer to read the credentials directly. Which of the following would be the BEST recommendation for storing and monitoring access to these shared credentials?

- A. TPM
- B. Local secure password file
- C. MFA
- D. Key vault

**Answer:** A

#### Explanation:

Reference: <https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/tpm-fundamentals>

#### NEW QUESTION 19

An organization's hunt team thinks a persistent threats exists and already has a foothold in the enterprise network. Which of the following techniques would be BEST for the hunt team to use to entice the adversary to uncover malicious activity?

- A. Deploy a SOAR tool.
- B. Modify user password history and length requirements.
- C. Apply new isolation and segmentation schemes.
- D. Implement decoy files on adjacent hosts.

**Answer:** C

#### Explanation:

Reference: <https://www.cynet.com/network-attacks/network-attacks-and-network-security-threats/>

#### NEW QUESTION 22

A security analyst is concerned that a malicious piece of code was downloaded on a Linux system. After some research, the analyst determines that the suspected piece of code is performing a lot of input/ output (I/O) on the disk drive.

Based on the output above, from which of the following process IDs can the analyst begin an investigation?

- A. 65
- B. 77
- C. 83
- D. 87

**Answer:** D

#### NEW QUESTION 27

A small company recently developed prototype technology for a military program. The company's security engineer is concerned about potential theft of the newly developed, proprietary information.

Which of the following should the security engineer do to BEST manage the threats proactively?

- A. Join an information-sharing community that is relevant to the company.
- B. Leverage the MITRE ATT&CK framework to map the TTR.
- C. Use OSINT techniques to evaluate and analyze the threats.
- D. Update security awareness training to address new threats, such as best practices for data security.

**Answer:** D

#### NEW QUESTION 32

A security analyst is reviewing the following output:

Which of the following would BEST mitigate this type of attack?

- A. Installing a network firewall
- B. Placing a WAF inline
- C. Implementing an IDS
- D. Deploying a honeypot

**Answer:** A

#### NEW QUESTION 37

A company is preparing to deploy a global service.

Which of the following must the company do to ensure GDPR compliance? (Choose two.)

- A. Inform users regarding what data is stored.

- B. Provide opt-in/out for marketing messages.
- C. Provide data deletion capabilities.
- D. Provide optional data encryption.
- E. Grant data access to third parties.
- F. Provide alternative authentication techniques.

**Answer:** AB

**Explanation:**

Reference: <https://gdpr.eu/compliance-checklist-us-companies/>

**NEW QUESTION 40**

An organization is designing a network architecture that must meet the following requirements: Users will only be able to access predefined services. Each user will have a unique allow list defined for access. The system will construct one-to-one subject/object access paths dynamically. Which of the following architectural designs should the organization use to meet these requirements?

- A. Peer-to-peer secure communications enabled by mobile applications
- B. Proxied application data connections enabled by API gateways
- C. Microsegmentation enabled by software-defined networking
- D. VLANs enabled by network infrastructure devices

**Answer:** C

**NEW QUESTION 41**

An application server was recently upgraded to prefer TLS 1.3, and now users are unable to connect their clients to the server. Attempts to reproduce the error are confirmed, and clients are reporting the following:  
ERR\_SSL\_VERSION\_OR\_CIPHER\_MISMATCH  
Which of the following is MOST likely the root cause?

- A. The client application is testing PFS.
- B. The client application is configured to use ECDHE.
- C. The client application is configured to use RC4.
- D. The client application is configured to use AES-256 in GCM.

**Answer:** C

**Explanation:**

Reference: [https://kinsta.com/knowledgebase/err\\_ssl\\_version\\_or\\_cipher\\_mismatch/](https://kinsta.com/knowledgebase/err_ssl_version_or_cipher_mismatch/)

#### NEW QUESTION 44

A university issues badges through a homegrown identity management system to all staff and students. Each week during the summer, temporary summer school students arrive and need to be issued a badge to access minimal campus resources.

The security team received a report from an outside auditor indicating the homegrown system is not consistent with best practices in the security field and leaves the institution vulnerable.

Which of the following should the security team recommend FIRST?

- A. Investigating a potential threat identified in logs related to the identity management system
- B. Updating the identity management system to use discretionary access control
- C. Beginning research on two-factor authentication to later introduce into the identity management system
- D. Working with procurement and creating a requirements document to select a new IAM system/vendor

**Answer:** A

#### NEW QUESTION 48

A satellite communications ISP frequently experiences outages and degraded modes of operation over one of its legacy satellite links due to the use of deprecated hardware and software. Three days per week, on average, a contracted company must follow a checklist of 16 different high-latency commands that must be run in serial to restore nominal performance. The ISP wants this process to be automated.

Which of the following techniques would be BEST suited for this requirement?

- A. Deploy SOAR utilities and runbooks.
- B. Replace the associated hardware.
- C. Provide the contractors with direct access to satellite telemetry data.
- D. Reduce link latency on the affected ground and satellite segments.

**Answer:** A

#### NEW QUESTION 50

A company plans to build an entirely remote workforce that utilizes a cloud-based infrastructure. The Chief Information Security Officer asks the security engineer to design connectivity to meet the following requirements:

Only users with corporate-owned devices can directly access servers hosted by the cloud provider. The company can control what SaaS applications each individual user can access. User browser activity can be monitored.

Which of the following solutions would BEST meet these requirements?

- A. IAM gateway, MDM, and reverse proxy
- B. VPN, CASB, and secure web gateway
- C. SSL tunnel, DLP, and host-based firewall
- D. API gateway, UEM, and forward proxy

**Answer:** B

#### NEW QUESTION 54

An organization recently experienced a ransomware attack. The security team leader is concerned about the attack reoccurring. However, no further security measures have been implemented.

Which of the following processes can be used to identify potential prevention recommendations?

- A. Detection
- B. Remediation
- C. Preparation
- D. Recovery

**Answer:** A

#### NEW QUESTION 56

An organization is preparing to migrate its production environment systems from an on-premises environment to a cloud service. The lead security architect is concerned that the organization's current methods for addressing risk may not be possible in the cloud environment.

Which of the following BEST describes the reason why traditional methods of addressing risk may not be possible in the cloud?

- A. Migrating operations assumes the acceptance of all risk.
- B. Cloud providers are unable to avoid risk.
- C. Specific risks cannot be transferred to the cloud provider.
- D. Risks to data in the cloud cannot be mitigated.

**Answer:** C

#### Explanation:

Reference: <https://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf>

#### NEW QUESTION 58

After a security incident, a network security engineer discovers that a portion of the company's sensitive external traffic has been redirected through a secondary ISP that is not normally used.

Which of the following would BEST secure the routes while allowing the network to function in the event of a single provider failure?

- A. Disable BGP and implement a single static route for each internal network.
- B. Implement a BGP route reflector.
- C. Implement an inbound BGP prefix list.
- D. Disable BGP and implement OSPF.

Answer: B

#### NEW QUESTION 60

A security engineer needs to recommend a solution that will meet the following requirements: Identify sensitive data in the provider's network  
Maintain compliance with company and regulatory guidelines  
Detect and respond to insider threats, privileged user threats, and compromised accounts Enforce datacentric security, such as encryption, tokenization, and access control Which of the following solutions should the security engineer recommend to address these requirements?

- A. WAF
- B. CASB
- C. SWG
- D. DLP

Answer: A

#### NEW QUESTION 64

A company that all mobile devices be encrypted, commensurate with the full disk encryption scheme of assets, such as workstation, servers, and laptops.  
Which of the following will MOST likely be a limiting factor when selecting mobile device managers for the company?

- A. Increased network latency
- B. Unavailable of key escrow
- C. Inability to selected AES-256 encryption
- D. Removal of user authentication requirements

Answer: A

#### NEW QUESTION 67

An application developer is including third-party background security fixes in an application. The fixes seem to resolve a currently identified security issue. However, when the application is released to the public, report come In that a previously vulnerability has returned .  
Which of the following should the developer integrate into the process to BEST prevent this type of behavior?

- A. Peer review
- B. Regression testing
- C. User acceptance
- D. Dynamic analysis

Answer: A

#### NEW QUESTION 70

The Chief information Officer (CIO) wants to establish a non-binding agreement with a third party that outlines the objectives of the mutual arrangement dealing with data transfers between both organizations before establishing a format partnership .  
Which of the follow would MOST likely be used?

- A. MOU
- B. OLA
- C. NDA
- D. SLA

Answer: A

#### NEW QUESTION 72

A developer implement the following code snippet.

Which of the following vulnerabilities does the code snippet resolve?

- A. SQL inject
- B. Buffer overflow
- C. Missing session limit
- D. Information leakage

Answer: D

#### NEW QUESTION 77

A security analyst is investigating a series of suspicious emails by employees to the security team. The email appear to come from a current business partner and do not contain images or URLs. No images or URLs were stripped from the message by the security tools the company uses instead, the emails only include the following in plain text.

Which of the following should the security analyst perform?

- A. Contact the security department at the business partner and alert them to the email event.
- B. Block the IP address for the business partner at the perimeter firewall.
- C. Pull the devices of the affected employees from the network in case they are infected with a zero-day virus.
- D. Configure the email gateway to automatically quarantine all messages originating from the business partner.

Answer: A

**NEW QUESTION 78**

Company A is establishing a contractual with Company B. The terms of the agreement are formalized in a document covering the payment terms, limitation of liability, and intellectual property rights .

Which of the following documents will MOST likely contain these elements?

- A. Company A-B SLA v2.docx
- B. Company A OLA v1b.docx
- C. Company A MSA v3.docx
- D. Company A MOU v1.docx
- E. Company A-B NDA v03.docx

**Answer:** A

**NEW QUESTION 82**

The Chief information Officer (CIO) asks the system administrator to improve email security at the company based on the following requirements:

- \* Transaction being requested by unauthorized individuals.
- \* Complete discretion regarding client names, account numbers, and investment information.
- \* Malicious attackers using email to malware and ransomware.
- \* Exfiltration of sensitive company information.

The cloud-based email solution will provide anti-malware reputation-based scanning, signature-based scanning, and sandboxing .

Which of the following is the BEST option to resolve the board's concerns for this email migration?

- A. Data loss prevention
- B. Endpoint detection response
- C. SSL VPN
- D. Application whitelisting

**Answer:** A

**NEW QUESTION 84**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CAS-004 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CAS-004 Product From:

<https://www.2passeasy.com/dumps/CAS-004/>

## Money Back Guarantee

### **CAS-004 Practice Exam Features:**

- \* CAS-004 Questions and Answers Updated Frequently
- \* CAS-004 Practice Questions Verified by Expert Senior Certified Staff
- \* CAS-004 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* CAS-004 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year