

CAS-004 Dumps

CompTIA Advanced Security Practitioner (CASP+) Exam

<https://www.certleader.com/CAS-004-dumps.html>



NEW QUESTION 1

Which of the following are risks associated with vendor lock-in? (Choose two.)

- A. The client can seamlessly move data.
- B. The vendor can change product offerings.
- C. The client receives a sufficient level of service.
- D. The client experiences decreased quality of service.
- E. The client can leverage a multicloud approach.
- F. The client experiences increased interoperability.

Answer: BD

Explanation:

Reference: <https://www.cloudflare.com/learning/cloud/what-is-vendor-lockin/#:~:text=Vendor%20lock%2Din%20can%20become,may%20involve%20reformatting%20the%20data>

NEW QUESTION 2

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 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

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 5

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 6

A SOC analyst is reviewing malicious activity on an external, exposed web server. During the investigation, the analyst determines specific traffic is not being logged, and there is no visibility from the WAF for the web application.

Which of the following is the MOST likely cause?

- A. The user agent client is not compatible with the WAF.
- B. A certificate on the WAF is expired.
- C. HTTP traffic is not forwarding to HTTPS to decrypt.
- D. Old, vulnerable cipher suites are still being used.

Answer: B

Explanation:

Reference: <https://aws.amazon.com/premiumsupport/knowledge-center/waf-block-http-requests-no-user-agent/>

NEW QUESTION 7

An organization is referencing NIST best practices for BCP creation while reviewing current internal organizational processes for mission-essential items. Which of the following phases establishes the identification and prioritization of critical systems and functions?

- A. Review a recent gap analysis.
- B. Perform a cost-benefit analysis.
- C. Conduct a business impact analysis.
- D. Develop an exposure factor matrix.

Answer: C

Explanation:

Reference: <https://itsm.ucsf.edu/business-impact-analysis-bia-0>

NEW QUESTION 8

A security engineer thinks the development team has been hard-coding sensitive environment variables in its code. Which of the following would BEST secure the company's CI/CD pipeline?

- A. Utilizing a trusted secrets manager
- B. Performing DAST on a weekly basis
- C. Introducing the use of container orchestration
- D. Deploying instance tagging

Answer: A

Explanation:

Reference: <https://about.gitlab.com/blog/2021/04/09/demystifying-ci-cd-variables/>

NEW QUESTION 9

A junior developer is informed about the impact of new malware on an Advanced RISC Machine (ARM) CPU, and the code must be fixed accordingly. Based on the debug, the malware is able to insert itself in another process memory location.

Which of the following technologies can the developer enable on the ARM architecture to prevent this type of malware?

- A. Execute never
- B. No-execute
- C. Total memory encryption
- D. Virtual memory encryption

Answer: A

Explanation:

Reference: <https://developer.arm.com/documentation/102433/0100/Stack-smashing-and-execution-permissions>

NEW QUESTION 10

A company is implementing SSL inspection. During the next six months, multiple web applications that will be separated out with subdomains will be deployed. Which of the following will allow the inspection of the data without multiple certificate deployments?

- A. Include all available cipher suites.
- B. Create a wildcard certificate.
- C. Use a third-party CA.
- D. Implement certificate pinning.

Answer: D

NEW QUESTION 10

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 14

A customer reports being unable to connect to a website at www.test.com to consume services. The customer notices the web application has the following published cipher suite:

Which of the following is the MOST likely cause of the customer's inability to connect?

- A. Weak ciphers are being used.
- B. The public key should be using ECDSA.
- C. The default should be on port 80.
- D. The server name should be test.com.

Answer: B

Explanation:

Reference: <https://security.stackexchange.com/questions/23383/ssh-key-type-rsa-dsa-ecdsa-are-there-easy-answers-forwhich-to-choose-when>

NEW QUESTION 19

A company is migrating from company-owned phones to a BYOD strategy for mobile devices. The pilot program will start with the executive management team and be rolled out to the rest of the staff in phases. The company's Chief Financial Officer loses a phone multiple times a year. Which of the following will MOST likely secure the data on the lost device?

- A. Require a VPN to be active to access company data.
- B. Set up different profiles based on the person's risk.
- C. Remotely wipe the device.
- D. Require MFA to access company applications.

Answer: D

NEW QUESTION 22

A Chief Information Officer is considering migrating all company data to the cloud to save money on expensive SAN storage. Which of the following is a security concern that will MOST likely need to be addressed during migration?

- A. Latency
- B. Data exposure
- C. Data loss
- D. Data dispersion

Answer: A

NEW QUESTION 24

A security analyst is performing a vulnerability assessment on behalf of a client. The analyst must define what constitutes a risk to the organization. Which of the following should be the analyst's FIRST action?

- A. Create a full inventory of information and data assets.
- B. Ascertain the impact of an attack on the availability of crucial resources.
- C. Determine which security compliance standards should be followed.
- D. Perform a full system penetration test to determine the vulnerabilities.

Answer: C

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 34

A company is looking to fortify its cybersecurity defenses and is focusing on its network infrastructure. The solution cannot affect the availability of the company's services to ensure false positives do not drop legitimate traffic.

Which of the following would satisfy the requirement?

- A. NIDS
- B. NIPS
- C. WAF
- D. Reverse proxy

Answer: B

Explanation:

Reference: <https://subscription.packtpub.com/book/networking-and-servers/9781782174905/5/ch05lv1sec38/differentiatingbetween-nids-and-nips>

NEW QUESTION 35

While investigating a security event, an analyst finds evidence that a user opened an email attachment from an unknown source. Shortly after the user opened the attachment, a group of servers experienced a large amount of network and resource activity. Upon investigating the servers, the analyst discovers the servers were encrypted by ransomware that is demanding payment within 48 hours or all data will be destroyed. The company has no response plans for ransomware. Which of the following is the NEXT step the analyst should take after reporting the incident to the management team?

- A. Pay the ransom within 48 hours.
- B. Isolate the servers to prevent the spread.

- C. Notify law enforcement.
- D. Request that the affected servers be restored immediately.

Answer: C

NEW QUESTION 37

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 41

A company has hired a security architect to address several service outages on the endpoints due to new malware. The Chief Executive Officer's laptop was impacted while working from home. The goal is to prevent further endpoint disruption.

The edge network is protected by a web proxy.

Which of the following solutions should the security architect recommend?

- A. Replace the current antivirus with an EDR solution.
- B. Remove the web proxy and install a UTM appliance.
- C. Implement a deny list feature on the endpoints.
- D. Add a firewall module on the current antivirus solution.

Answer: C

NEW QUESTION 45

DRAG DROP

An organization is planning for disaster recovery and continuity of operations. INSTRUCTIONS

Review the following scenarios and instructions. Match each relevant finding to the affected host.

After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective action for that finding. Each finding may be used more than once.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button. Select and Place:

A.

A.

Answer: A

NEW QUESTION 50

A business stores personal client data of individuals residing in the EU in order to process requests for mortgage loan approvals. Which of the following does the business's IT manager need to consider?

- A. The availability of personal data
- B. The right to personal data erasure
- C. The company's annual revenue
- D. The language of the web application

Answer: B

Explanation:

Reference: <https://gdpr.eu/right-to-beforgotten/#:~:text=Also%20known%20as%20the%20right,to%20delete%20their%20personal%20data.&text=The%20General%20Data%20Protection%20Regulation,collected%2C%20processed%2C%20and%20erased>

NEW QUESTION 54

An organization wants to perform a scan of all its systems against best practice security configurations.

Which of the following SCAP standards, when combined, will enable the organization to view each of the configuration checks in a machine-readable checklist format for fill automation? (Choose two.)

- A. ARF
- B. XCCDF
- C. CPE
- D. CVE
- E. CVSS
- F. OVAL

Answer: BF

Explanation:

Reference: <https://www.govinfo.gov/content/pkg/GOVPUB-C13-9ecd8eae582935c93d7f410e955dabb6/pdf/GOVPUB-C13-9ecd8eae582935c93d7f410e955dabb6.pdf> (p.12)

NEW QUESTION 55

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 58

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 63

A company's claims processed department has a mobile workforce that receives a large number of email submissions from personal email addresses. An employees recently received an email that appeared to be claim form, but it installed malicious software on the employee's laptop when was opened.

- A. Implement application whitelisting and add only the email client to the whitelist for laptop in the claims processing department.
- B. Required all laptops to connect to the VPN before accessing email.
- C. Implement cloud-based content filtering with sandboxing capabilities.
- D. Install a mail gateway to scan incoming messages and strip attachments before they reach the mailbox.

Answer: C

NEW QUESTION 64

A company is repeatedly being breached by hackers who valid credentials. The company's Chief information Security Officer (CISO) has installed multiple controls for authenticating users, including biometric and token-based factors. Each successive control has increased overhead and complexity but has failed to stop further breaches. An external consultant is evaluating the process currently in place to support the authentication controls .
Which of the following recommendation would MOST likely reduce the risk of unauthorized access?

- A. Implement strict three-factor authentication.
- B. Implement least privilege policies
- C. Switch to one-time or all user authorizations.
- D. Strengthen identify-proofing procedures

Answer: A

NEW QUESTION 68

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CAS-004 Exam with Our Prep Materials Via below:

<https://www.certleader.com/CAS-004-dumps.html>