

Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

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



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 security analyst is researching containerization concepts for an organization. The analyst is concerned about potential resource exhaustion scenarios on the Docker host due to a single application that is overconsuming available resources.

Which of the following core Linux concepts BEST reflects the ability to limit resource allocation to containers?

- A. Union filesystem overlay
- B. Cgroups
- C. Linux namespaces
- D. Device mapper

Answer: B

Explanation:

Reference: <https://www.ibm.com/support/pages/deep-dive-yarn-cgroups-hadoop-dev>

NEW QUESTION 3

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 4

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 5

A security architect works for a manufacturing organization that has many different branch offices. The architect is looking for a way to reduce traffic and ensure the branch offices receive the latest copy of revoked certificates issued by the CA at the organization's headquarters location. The solution must also have the lowest power requirement on the CA.

Which of the following is the BEST solution?

- A. Deploy an RA on each branch office.
- B. Use Delta CRLs at the branches.
- C. Configure clients to use OCSP.
- D. Send the new CRLs by using GPO.

Answer: C

Explanation:

Reference: <https://www.sciencedirect.com/topics/computer-science/revoke-certificate>

NEW QUESTION 6

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 7

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 8

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 9

A company's SOC has received threat intelligence about an active campaign utilizing a specific vulnerability. The company would like to determine whether it is vulnerable to this active campaign.

Which of the following should the company use to make this determination?

- A. Threat hunting
- B. A system penetration test
- C. Log analysis within the SIEM tool
- D. The Cyber Kill Chain

Answer: B

NEW QUESTION 10

A shipping company that is trying to eliminate entire classes of threats is developing an SELinux policy to ensure its custom Android devices are used exclusively for package tracking.

After compiling and implementing the policy, in which of the following modes must the company ensure the devices are configured to run?

- A. Protecting
- B. Permissive
- C. Enforcing
- D. Mandatory

Answer: B

Explanation:

Reference: <https://source.android.com/security/selinux/customize>

NEW QUESTION 10

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 11

A security engineer needs to implement a solution to increase the security posture of user endpoints by providing more visibility and control over local administrator accounts. The endpoint security team is overwhelmed with alerts and wants a solution that has minimal operational burdens. Additionally, the solution must maintain a positive user experience after implementation.

Which of the following is the BEST solution to meet these objectives?

- A. Implement Privileged Access Management (PAM), keep users in the local administrators group, and enable local administrator account monitoring.
- B. Implement PAM, remove users from the local administrators group, and prompt users for explicit approval when elevated privileges are required.
- C. Implement EDR, remove users from the local administrators group, and enable privilege escalation monitoring.
- D. Implement EDR, keep users in the local administrators group, and enable user behavior analytics.

Answer: A

Explanation:

Reference: <https://www.cyberark.com/what-is/privileged-access-management/>

NEW QUESTION 13

A technician is reviewing the logs and notices a large number of files were transferred to remote sites over the course of three months. This activity then stopped. The files were transferred via TLSprotected HTTP sessions from systems that do not send traffic to those sites.

The technician will define this threat as:

- A. a decrypting RSA using obsolete and weakened encryption attack.
- B. a zero-day attack.
- C. an advanced persistent threat.

D. an on-path attack.

Answer: A

Explanation:

Reference: <https://www.internetsociety.org/deploy360/tls/basics/>

NEW QUESTION 17

A developer wants to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users. Which of the following would be BEST for the developer to perform? (Choose two.)

- A. Utilize code signing by a trusted third party.
- B. Implement certificate-based authentication.
- C. Verify MD5 hashes.
- D. Compress the program with a password.
- E. Encrypt with 3DES.
- F. Make the DACL read-only.

Answer: AB

NEW QUESTION 20

A new web server must comply with new secure-by-design principles and PCI DSS. This includes mitigating the risk of an on-path attack. A security analyst is reviewing the following web server configuration:

Which of the following ciphers should the security analyst remove to support the business requirements?

- A. TLS_AES_128_CCM_8_SHA256
- B. TLS_DHE_DSS_WITH_RC4_128_SHA
- C. TLS_CHACHA20_POLY1305_SHA256
- D. TLS_AES_128_GCM_SHA256

Answer: C

NEW QUESTION 22

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 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 30

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 34

Which of the following allows computation and analysis of data within a ciphertext without knowledge of the plaintext?

- A. Lattice-based cryptography
- B. Quantum computing
- C. Asymmetric cryptography
- D. Homomorphic encryption

Answer: C

Explanation:

Reference: <https://searchsecurity.techtarget.com/definition/cryptanalysis>

NEW QUESTION 36

A security analyst is investigating a possible buffer overflow attack. The following output was found on a user's workstation: `graphic.linux_randomization.prg`
Which of the following technologies would mitigate the manipulation of memory segments?

- A. NX bit
- B. ASLR
- C. DEP
- D. HSM

Answer: B

Explanation:

Reference: <http://webpages.eng.wayne.edu/~fy8421/19sp-csc5290/labs/lab2-instruction.pdf> (3)

NEW QUESTION 39

An organization is considering a BYOD standard to support remote working. The first iteration of the solution will utilize only approved collaboration applications and the ability to move corporate data between those applications. The security team has concerns about the following:

Unstructured data being exfiltrated after an employee leaves the organization

Data being exfiltrated as a result of compromised credentials

Sensitive information in emails being exfiltrated

Which of the following solutions should the security team implement to mitigate the risk of data loss?

- A. Mobile device management, remote wipe, and data loss detection
- B. Conditional access, DoH, and full disk encryption
- C. Mobile application management, MFA, and DRM
- D. Certificates, DLP, and geofencing

Answer: A

NEW QUESTION 43

A network architect is designing a new SD-WAN architecture to connect all local sites to a central hub site. The hub is then responsible for redirecting traffic to public cloud and datacenter applications. The SD-WAN routers are managed through a SaaS, and the same security policy is applied to staff whether working in the office or at a remote location. The main requirements are the following:

* 1. The network supports core applications that have 99.99% uptime.

* 2. Configuration updates to the SD-WAN routers can only be initiated from the management service.

* 3. Documents downloaded from websites must be scanned for malware.

Which of the following solutions should the network architect implement to meet the requirements?

- A. Reverse proxy, stateful firewalls, and VPNs at the local sites
- B. IDSs, WAFs, and forward proxy IDS
- C. DoS protection at the hub site, mutual certificate authentication, and cloud proxy
- D. IPSs at the hub, Layer 4 firewalls, and DLP

Answer: B

NEW QUESTION 47

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 48

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 52

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 56

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 60

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 65

A health company has reached the physical and computing capabilities in its datacenter, but the computing demand continues to increase. The infrastructure is fully virtualized and runs custom and commercial healthcare application that process sensitive health and payment information .

Which of the following should the company implement to ensure it can meet the computing demand while complying with healthcare standard for virtualization and cloud computing?

- A. Hybrid IaaS solution in a single-tenancy cloud
- B. PaaS solution in a multi-tenancy cloud
- C. SaaS solution in a community cloud
- D. Private SaaS solution in a single-tenancy cloud.

Answer: D

NEW QUESTION 68

Over the last 90 days, many storage services has been exposed in the cloud services environments, and the security team does not have the ability to see is creating these instance. Shadow IT is creating data services and instances faster than the small security team can keep up with them. The Chief information security Officer (CIASO) has asked the security officer (CISO) has asked the security lead architect to architect to recommend solutions to this problem. Which of the following BEST addresses the problem best address the problem with the least amount of administrative effort?

- A. Compile a list of firewall requests and compare than against interesting cloud services.
- B. Implement a CASB solution and track cloud service use cases for greater visibility.
- C. Implement a user-behavior system to associate user events and cloud service creation events.
- D. Capture all log and feed then to a SIEM and then for cloud service events

Answer: C

NEW QUESTION 70

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 71

Ann, a CIRT member, is conducting incident response activities on a network that consists of several hundred virtual servers and thousands of endpoints and users. The network generates more than 10,000 log messages per second. The enterprise belong to a large, web-based cryptocurrency startup, Ann has distilled the relevant information into an easily digestible report for executive management. However, she still needs to collect evidence of the intrusion that caused the incident .

Which of the following should Ann use to gather the required information?

- A. Traffic interceptor log analysis
- B. Log reduction and visualization tools
- C. Proof of work analysis
- D. Ledger analysis software

Answer: B

NEW QUESTION 74

.....

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