Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

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

NEW QUESTION 1
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 2
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 3
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 4
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 5
Due to locality and budget constraints, an organization's satellite office has a lower bandwidth allocation than other offices in the organization. As a result, the local security infrastructure staff is assessing architectural options that will help preserve network bandwidth and increase speed to both internal and external resources while not sacrificing threat visibility.
Which of the following would be the BEST option to implement?

A. Distributed connection allocation
B. Local caching
C. Content delivery network
D. SD-WAN vertical heterogeneity

Answer: C

NEW QUESTION 6
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 7
A vulnerability analyst identified a zero-day vulnerability in a company's internally developed software. Since the current vulnerability management system does not have any checks for this vulnerability, an engineer has been asked to create one.
Which of the following would be BEST suited to meet these requirements?

A. ARF
B. ISACs
C. Node.js
D. OVAL

Answer: D

NEW QUESTION 8
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 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 developer is creating a new mobile application for a company. The application uses REST API and TLS 1.2 to communicate securely with the external back- end server. Due to this configuration, the company is concerned about HTTPS interception attacks.
Which of the following would be the BEST solution against this type of attack?

A. Cookies
B. Wildcard certificates
C. HSTS
D. Certificate pinning

Answer: C

Explanation:
Reference: https://cloud.google.com/security/encryption-in-transit

ALTS has a secure handshake protocol similar to mutual TLS. Two services wishing to communicate using ALTS employ this handshake protocol to authenticate and negotiate communication parameters before sending any sensitive information. The protocol is a two-step process:

- **Step 1:Handshake** The client initiates an elliptic curve-Diffie Hellman (ECDH) handshake with the server using Curve25519. The client and server each have certified ECDH public parameters as part of their certificate, which is used during a Diffie Hellman key exchange. The handshake results in a common traffic key that is available on the client and the server. The peer identities from the certificates are surfaced to the application layer to use in authorization decisions.
- **Step 2: Record encryption** Using the common traffic key from Step 1, data is transmitted from the client to the server securely. Encryption in ALTS is implemented using BoringSSL and other encryption libraries. Encryption is most commonly AES 128-GCM while integrity is provided by AES-GCM's GMAC

NEW QUESTION 10
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 12
A security analyst discovered that the company's WAF was not properly configured. The main web server was breached, and the following payload was found in one of the malicious requests:

```
<!DOCTYPE doc [
<!ELEMENT doc ANY>
<ENTITY xxe SYSTEM "file:///etc/password">]>
<doc>&xxe;</doc>
```

Which of the following would BEST mitigate this vulnerability?

A. CAPTCHA
B. Input validation
C. Data encoding
D. Network intrusion prevention

Answer: B

Explanation:
Reference: https://hdivsecurity.com/owasp-xml-external-entities-xxe

Example #1: The attacker attempts to extract data from the server

```
<?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE foo [
<!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]> <foo>&xxe;</foo>
```

Example #2: An attacker probes the server's private network by changing the above ENTITY line to

```
<!ENTITY xxe SYSTEM "https://192.168.1.1/private" >]>
```

NEW QUESTION 17
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 20
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.

```
procs ---------memory--------swap--io--  --system-- -----cpu------
r b swpd free  buff   cache  si so bi     bo          in  cs   us sy id wa st
3 0 0    44712 110052 623096 0  0  304023 30004040    217 883  13 3  83 1  0
1 0 0    44408 110052 623096 0  0  300    200003      88  1446 31 4  65 0  0
0 0 0    44524 110052 623096 0  0  400020 20          84  872  11 2  87 0  0
0 2 0    44516 110052 623096 0  0  10     0           149 142  18 5  77 0  0
0 0 0    44524 110052 623096 0  0  0      0           60  431  14 1  85 0  0
```

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 24
All staff at a company have started working remotely due to a global pandemic. To transition to remote work, the company has migrated to SaaS collaboration tools. The human resources department wants to use these tools to process sensitive information but is concerned the data could be:
Leaked to the media via printing of the documents Sent to a personal email address
Accessed and viewed by systems administrators Uploaded to a file storage site Which of the following would mitigate the department's concerns?

A. Data loss detection, reverse proxy, EDR, and PGP
B. VDI, proxy, CASB, and DRM
C. Watermarking, forward proxy, DLP, and MFA
D. Proxy, secure VPN, endpoint encryption, and AV

Answer: B

NEW QUESTION 28
A security engineer was auditing an organization's current software development practice and discovered that multiple opensource libraries were Integrated into the organization's software. The organization currently performs SAST and DAST on the software it develops.
Which of the following should the organization incorporate into the SDLC to ensure the security of the open-source libraries?

A. Perform additional SAST/DAST on the open-source libraries.
B. Implement the SDLC security guidelines.
C. Track the library versions and monitor the CVE website for related vulnerabilities.
D. Perform unit testing of the open-source libraries.

Answer: B

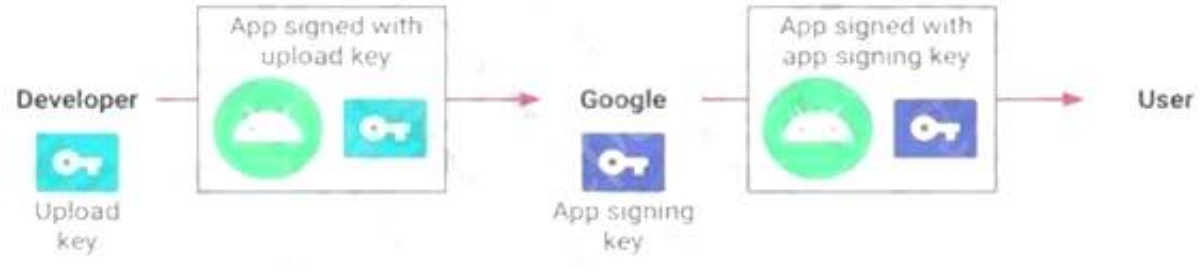
Explanation:
Reference: https://www.whitesourcesoftware.com/resources/blog/application-security-best-practices/

NEW QUESTION 29
A company publishes several APIs for customers and is required to use keys to segregate customer data sets. Which of the following would be BEST to use to store customer keys?

A. A trusted platform module
B. A hardware security module
C. A localized key store
D. A public key infrastructure

Answer: C

Explanation:
Reference: https://developer.android.com/studio/publish/app-signing



NEW QUESTION 32
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 36
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 39
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 40
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. Pass solution in a multinency cloud
C. SaaS solution in a community cloud
D. Private SaaS solution in a single tenancy cloud.

Answer: D

NEW QUESTION 43
A developer implement the following code snippet.

```
catch (Exception e)
{
   if(log.isDebugEnabled())
   {
      log.debug("Caught InvalidDNException Exception --"
      + e.toString());
   }
}
```

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 47
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 49
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 50
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 52
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 approved to be claim form, but it installed malicious software on the employee’s laptop when was opened.

A. Impalement 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 53
.....

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