CompTIA

Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

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
A security architect is implementing a web application that uses a database back end. Prior to the production, the architect is concerned about the possibility of XSS attacks and wants to identify security controls that could be put in place to prevent these attacks.
Which of the following sources could the architect consult to address this security concern?

A. SDLC
B. OVAL
C. IEEE
D. OWASP

Answer: B

Explanation:
Reference: https://dzone.com/articles/what-is-oval-a-community-driven-vulnerability-mana

NEW QUESTION 4
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/

First, create the regex pattern set:

1. Open the AWS WAF console.
2. In the navigation pane, under **AWS WAF**, choose **Regex pattern sets**.
3. For **Region**, select the Region where you created your web access control list (web ACL).
   Note: Select **Global** if your web ACL is set up for Amazon CloudFront.
4. Choose **Create regex pattern sets**.
5. For **Regex pattern set name**, enter **testpattern**.
6. For **Regular expressions**, enter **.+**
7. Choose **Create regex pattern set**.

NEW QUESTION 5

An organization recently started processing, transmitting, and storing its customers' credit card information. Within a week of doing so, the organization suffered a massive breach that resulted in the exposure of the customers' information.
Which of the following provides the BEST guidance for protecting such information while it is at rest and in transit?

A. NIST
B. GDPR
C. PCI DSS
D. ISO

Answer: C

Explanation:
Reference: https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

NEW QUESTION 6
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 7
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

1. Use the latest Android kernel.
2. Adopt the principle of least privilege.
3. Address only your own additions to Android. The default policy works with the Android Open Source Project codebase automatically.
4. Compartmentalize software components into modules that conduct singular tasks.
5. Create SELinux policies that isolate those tasks from unrelated functions.
6. Put those policies in `*.te` files (the extension for SELinux policy source files) within the `/device/manufacturer/device-name/sepolicy` directory and use `BOARD_SEPOLICY` variables to include them in your build.
7. Make new domains permissive initially. This is done by using a permissive declaration in the domain's `.te` file.
8. Analyze results and refine your domain definitions.
9. Remove the permissive declaration when no further denials appear in userdebug builds.

NEW QUESTION 8
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 9
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 10
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 10
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 13
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/

- Conduct an information audit for EU personal data

Confirm that your organization needs to comply with the GDPR. First, determine what personal data you process and whether any of it belongs to people in the EU. If you do process such data, determine whether "the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment." Recital 23 can help you clarify whether your activities qualify as subject to the GDPR. If you are subject to the GDPR, continue to the next steps.

- Inform your customers why you're processing their data

NEW QUESTION 18
An energy company is required to report the average pressure of natural gas used over the past quarter. A PLC sends data to a historian server that creates the required reports.
Which of the following historian server locations will allow the business to get the required reports in an ?? and IT environment?

A. In the ?? environment, use a VPN from the IT environment into the ?? environment.
B. In the ?? environment, allow IT traffic into the ?? environment.
C. In the IT environment, allow PLCs to send data from the ?? environment to the IT environment.
D. Use a screened subnet between the ?? and IT environments.

Answer: A

NEW QUESTION 20
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 22
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

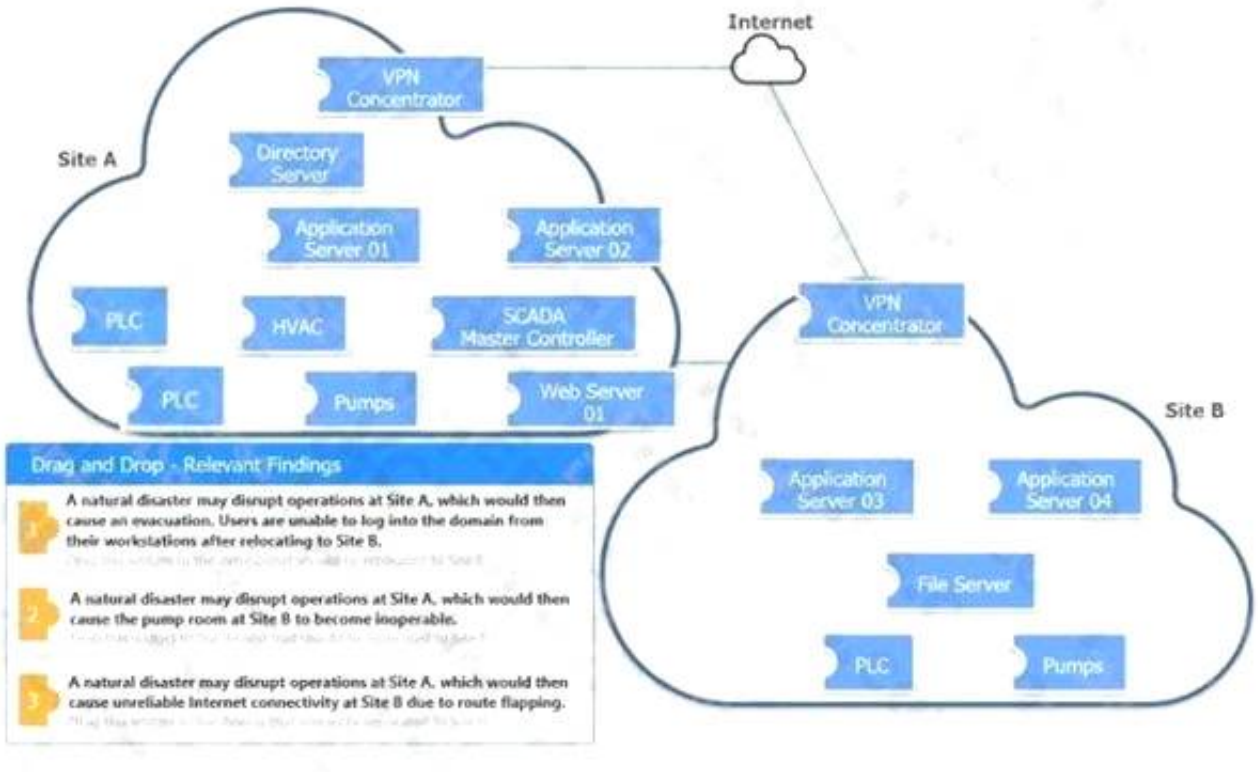
NEW QUESTION 26
Clients are reporting slowness when attempting to access a series of load-balanced APIs that do not require authentication. The servers that host the APIs are showing heavy CPU utilization. No alerts are found on the WAFs sitting in front of the APIs. Which of the following should a security engineer recommend to BEST remedy the performance issues in a timely manner?

A. Implement rate limiting on the API.
B. Implement geoblocking on the WAF.
C. Implement OAuth 2.0 on the API.
D. Implement input validation on the API.

Answer: C

NEW QUESTION 30
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 33
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 35
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 39
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 43
The Chief information Officer (CIO) wants to establish a non-banding 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 44
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 48
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 52
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 53
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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