

CompTIA

Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam



NEW QUESTION 1

A security analyst receives an alert from the SIEM regarding unusual activity on an authorized public SSH jump server. To further investigate, the analyst pulls the event logs directly from /var/log/ auth.log: graphic.ssh_auth_log.

Which of the following actions would BEST address the potential risks by the activity in the logs?

- A. Alerting the misconfigured service account password
- B. Modifying the AllowUsers configuration directive
- C. Restricting external port 22 access
- D. Implementing host-key preferences

Answer: C

Explanation:

Reference: <https://www.rapid7.com/blog/post/2017/10/04/how-to-secure-ssh-server-using-port-knocking-on-ubuntu-linux/>

NEW QUESTION 2

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 3

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 4

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 5

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 6

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 7

A security analyst is reviewing network connectivity on a Linux workstation and examining the active TCP connections using the command line. Which of the following commands would be the BEST to run to view only active Internet connections?

- A. `sudo netstat -antu | grep "LISTEN" | awk '{print$5}'`
- B. `sudo netstat -nlt -p | grep "ESTABLISHED"`
- C. `sudo netstat -plntu | grep -v "Foreign Address"`
- D. `sudo netstat -pnut -w | column -t -s '$\w'`
- E. `sudo netstat -pnut | grep -P ^tcp`

Answer: B

Explanation:

Reference: <https://www.codegrepper.com/code-examples/shell/netstat+find+port>

NEW QUESTION 8

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 9

A security analyst is reviewing the following output:

```
Request URL: http://www.largeworldwidebank.org/../../../../etc/passwd
Request Method: GET
Status Code: 200 OK
Remote Address: 107.240.1.127:443
Content-Length: 1245
Content-Type: text/html
Date: Tue, 03 Nov 2020 19:47:14 GMT
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cache-Control: max-age=0
Connection: keep-alive
Host: www.largeworldwidebank.org/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36
```

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 10

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 10

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 14

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 16

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 20

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 21

Over the last 90 days, many storage services have been exposed in the cloud services environments, and the security team does not have the ability to see is creating these instances. Shadow IT is creating data services and instances faster than the small security team can keep up with them. The Chief information security Officer (CISO) 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 them 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 logs and feed them to a SIEM and then for cloud service events

Answer: C

NEW QUESTION 25

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 26

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 28

A small company needs to reduce its operating costs. vendors have proposed solutions, which all focus on management of the company's website and services. The Chief information Security Officer (CISO) insist all available resources in the proposal must be dedicated, but managing a private cloud is not an option . Which of the following is the BEST solution for this company?

- A. Community cloud service model
- B. Multitenancy SaaS
- C. Single-tenancy SaaS
- D. On-premises cloud service model

Answer: A

NEW QUESTION 31

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 32

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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

100% Actual & Verified — Instant Download, Please Click
[Order The CAS-004 Practice Test Here](#)