CAS-004 Q&As

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-004 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/cas-004.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A security review of the architecture for an application migration was recently completed. The following observations were made:

1.

External inbound access is blocked.

2.

A large amount of storage is available.

3.

Memory and CPU usage are low.

4.

The load balancer has only a single server assigned.

5.

Multiple APIs are integrated.

Which of the following needs to be addressed?

A. Scalability

B. Automation

C. Availability

D. Performance

Correct Answer: C

Ensuring availability typically involves having multiple servers or instances behind a load balancer to provide redundancy and failover capabilities. This approach enhances the system\\'s resilience, ensuring that services remain available even if one server experiences issues. Therefore, to improve availability, the architecture should include additional servers or instances to handle the traffic, thus preventing downtime in case of failure.

QUESTION 2

A networking team asked a security administrator to enable Flash on its web browser. The networking team explained that an important legacy embedded system gathers SNMP information from various devices. The system can only be managed through a web browser running Flash. The embedded system will be replaced within the year but is still critical at the moment.

Which of the following should the security administrator do to mitigate the risk?

A. Explain to the networking team the reason Flash is no longer available and insist the team move up the timetable for replacement.

B. Air gap the legacy system from the network and dedicate a laptop with an end-of-life OS on it to connect to the system via crossover cable for management.

C. Suggest that the networking team contact the original embedded system\\'s vendor to get an update to the system that does not require Flash.

D. Isolate the management interface to a private VLAN where a legacy browser in a VM can be used as needed to manage the system.

Correct Answer: D

QUESTION 3

The Chief Information Security Officer is concerned about the possibility of employees downloading malicious files from the internet and opening them on corporate workstations. Which of the following solutions would be BEST to reduce this risk?

A. Integrate the web proxy with threat intelligence feeds.

B. Scan all downloads using an antivirus engine on the web proxy.

C. Block known malware sites on the web proxy.

D. Execute the files in the sandbox on the web proxy.

Correct Answer: D

Sandboxing provides a proactive approach, evaluating files based on behavior and potentially catching malicious files that signature-based solutions might miss.

QUESTION 4

A security engineer is re-architecting a network environment that provides regional electric distribution services. During a pretransition baseline assessment, the engineer identified the following security-relevant characteristics of the environment:

1.

Enterprise IT servers and supervisory industrial systems share the same subnet.

2.

Supervisory controllers use the 750MHz band to direct a portion of fielded PLCs.

3.

Command and telemetry messages from industrial control systems are unencrypted and unauthenticated.

Which of the following re-architecture approaches would be best to reduce the company\\'s risk?

A. Implement a one-way guard between enterprise IT services and mission-critical systems, obfuscate legitimate RF signals by broadcasting noise, and implement modern protocols to authenticate ICS messages.

B. Characterize safety-critical versus non-safety-critical systems, isolate safety-critical systems from other systems, and increase the directionality of RF links in the field.

C. Create a new network segment for enterprise IT servers, configure NGFW to enforce a well-defined segmentation policy, and implement a WIDS to monitor the spectrum.

D. Segment supervisory controllers from field PLCs, disconnect the entire network from the internet, and use only the 750MHz link for controlling energy distribution services.

Correct Answer: C

The best approach to reduce the company\\'s risk is to segregate the enterprise IT servers and supervisory industrial systems. Creating a new network segment and using a Next- Generation Firewall (NGFW) to enforce a strict segmentation policy will help to isolate the systems and protect against potential attacks. Additionally, implementing a Wireless Intrusion Detection System (WIDS) can help monitor the spectrum for unauthorized devices or interference.

QUESTION 5

A company recently deployed an agent-based DLP solution to all laptop in the environment. The DLP solution is configured to restrict the following:

1.

USB ports

2.

FTP connections

3.

Access to cloud-based storage sites

4.

Outgoing email attachments

5.

Saving data on the local C: drive

6.

Despite these restrictions, highly confidential data was from a secure fileshare in the research department.

Which of the following should the security team implement FIRST?

A. Application whitelisting for all company-owned devices

B. A secure VDI environment for research department employees

C. NIDS/NIPS on the network segment used by the research department

D. Bluetooth restriction on all laptops

Correct Answer: A

QUESTION 6

A Chief information Security Officer (CISO) has launched to create a rebuts BCP/DR plan for the entire company. As part of the initiative , the security team must gather data supporting s operational importance for the applications used by the business and determine the order in which the application must be back online.

Which of the following be the FIRST step taken by the team?

A. Perform a review of all policies an procedures related to BGP a and DR and created an educated educational module that can be assigned to at employees to provide training on BCP/DR events.

B. Create an SLA for each application that states when the application will come back online and distribute this information to the business units.

C. Have each business unit conduct a BIA and categories the application according to the cumulative data gathered.

D. Implement replication of all servers and application data to back up detacenters that are geographically from the central datacenter and release an upload BPA to all clients.

Correct Answer: C

QUESTION 7

A university issues badges through a homegrown identity management system to all staff and students. Each week during the summer, temporary summer school students arrive and need to be issued a badge to access minimal campus resources. The security team received a report from an outside auditor indicating the homegrown system is not consistent with best practices in the security field and leaves the institution vulnerable.

Which of the following should the security team recommend FIRST?

A. Investigating a potential threat identified in logs related to the identity management system

B. Updating the identity management system to use discretionary access control

C. Beginning research on two-factor authentication to later introduce into the identity management system

D. Working with procurement and creating a requirements document to select a new IAM system/vendor

Correct Answer: A

QUESTION 8

city government\\'s IT director was notified by the City council that the following cybersecurity requirements must be met to be awarded a large federal grant:

Logs for all critical devices must be retained for 365 days to enable monitoring and threat hunting. All privileged user access must be tightly controlled and tracked to mitigate compromised accounts. Ransomware threats and zero-day

vulnerabilities must be quickly identified. Which of the following technologies would BEST satisfy these requirements? (Select THREE).

A. Endpoint protection

B. Log aggregator

C. Zero trust network access

D. PAM

E. Cloud sandbox

F. SIEM

G. NGFW

Correct Answer: BDF

Log aggregator: A log aggregator is a tool that collects, parses, and stores logs from various sources, such as devices, applications, servers, etc. A log aggregator can help meet the requirement of retaining logs for 365 days by providing a centralized and scalable storage solution1 . PAM: PAM stands for privileged access management. It is a technology that controls and monitors the access of privileged users (such as administrators) to critical systems and data. PAM can help meet the requirement of controlling and tracking privileged user access by enforcing policies such as least privilege, multifactor authentication, password rotation, session recording, etc. . SIEM: SIEM stands for security information and event management. It is a technology that analyzes and correlates logs from various sources to detect and respond to security incidents. SIEM can help meet the requirement of identifying ransomware threats and zero- day vulnerabilities by providing real-time alerts, threat intelligence feeds, incident response workflows, etc.

QUESTION 9

A Chief Information Security Officer (CISO) reviewed data from a cyber exercise that examined all aspects of the company\\'s response plan. Which of the following best describes what the CISO reviewed?

A. An after-action report

B. A tabletop exercise

C. A system security plan

D. A disaster recovery plan

Correct Answer: A

An after-action report is a document that summarizes the performance of a team during a cybersecurity incident. It is used to review all aspects of the incident response plan, including what was done correctly, what needs improvement, and how the team responded to the incident. The CISO\\'s review of data from a cyber exercise would typically result in an after-action report, which helps in improving future responses to incidents.

QUESTION 10

In a shared responsibility model for PaaS, which of the following is a customer\\'s responsibility?

A. Network security

B. Physical security

C. OS security

D. Host infrastructure

Correct Answer: C

QUESTION 11

A company has decided to move an ERP application to a public cloud vendor. The company wants to replicate some of its global policies from on premises to cloud. The policies include data encryption, token management, and limited user

access to the ERP application The Chief Information Officer (CIO) is mainly concerned about privileged accounts that might be compromised and used to alter data in the ERP application.

Which of the following is the BEST option to meet the requirements?

A. Sandboxing

B. CASB

C. MFA

D. Security as a service

Correct Answer: D

QUESTION 12

After installing an unapproved application on a personal device, a Chief Executive Officer reported an incident to a security analyst. This device is not controlled by the MDM solution, as stated in the BVOD policy. However, the device contained critical confidential information. The cyber incident response team performed the analysis on the device and found the following log:

Wed 12 Dec 2020 10:00:03 Unknown sources is now enabled on this device.

Which of the following is the MOST likely reason for the successful attack?

A. Lack of MDM controls

B. Auto-join hotspots enabled

C. Sideloading

D. Lack of application segmentation

Correct Answer: C

The enabling of "Unknown sources" suggests that an application was installed from outside the official app store, which can introduce significant security risks, especially if the source of the application isn\\'t trusted. This process is known as

sideloading.

QUESTION 13

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:

1.

Unstructured data being exfiltrated after an employee leaves the organization

2.

Data being exfiltrated as a result of compromised credentials

3.

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

Correct Answer: C

QUESTION 14

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

Correct Answer: E

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

QUESTION 15

A company recently migrated all its workloads to the cloud and implemented a transit VPC with a managed firewall. The cloud infrastructure implements a 10.0.0.0/16 network, and the firewall implements the following ACLs:

```
FROM UNTRUST TO TRUST
10 PERMIT TCP FROM 0.0.0.0/0 ANY TO 10.0.0.0/16 80,443
20 PERMIT TCP FROM 192.168.1.0/24 ANY TO 10.0.10.0/24 22

FROM TRUST TO UNTRUST
10 PERMIT IP FROM 10.0.0.0/16 ANY TO 0.0.0.0/0 ANY
```

The Chief Information Security Officer wants to monitor relevant traffic for signs of data exfiltration. Which of the following should the organization place in its monitoring tool to BEST detect data exfiltration while reducing log size and the time to search logs?

A. FROM UDP 10.0.0.0/16 ANY TO 0.0.0.0/0 ANY

B. FROM TCP 10.0.0.0/16 80,443 TO 0.0.0.0/0 ANY

C. FROM TCP 0.0.0.0/0 ANY TO 10.0.0.0/16 80,443,22

D. FROM IP 10.0.0.0/16 ANY TO 0.0.0.0/0 ANY

E. FROM IP 0.0.0.0/0 ANY TO TCP 0.0.0.0/0 ANY

F. FROM UDP 0.0.0.0/0 ANY TO 0.0.0.0/0 ANY

Correct Answer: B