CAS-004$^{Q\&As}$

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-004 Exam with 100% Guarantee

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

QUESTION 1

A client is adding scope to a project. Which of the following processes should be used when requesting updates or corrections to the client\\'s systems?

A. The implementation engineer requests direct approval from the systems engineer and the Chief Information Security Officer.

B. The change control board must review and approve a submission.

C. The information system security officer provides the systems engineer with the system updates.

D. The security engineer asks the project manager to review the updates for the client\\'s system.

Correct Answer: B

QUESTION 2

A risk assessment determined that company data was leaked to the general public during a migration. Which of the following best explains the root cause of this issue?

A. Incomplete firewall rules between the CSP and on-premises infrastructure

B. Insufficient logging of cloud activities to company SIEM

C. Failure to implement full disk encryption to on-premises data storage

D. Misconfiguration of access controls on cloud storage containers

Correct Answer: D

During a migration, data is often moved to cloud storage containers. If these containers are not properly configured, they may be accessible to the public or unauthorized users, leading to data leaks. Misconfigurations such as setting permissions to public or not restricting access appropriately are common causes of data breaches in cloud environments.

QUESTION 3

Which of the following is the MOST likely reason an organization would decide to use a BYOD policy?

A. It enables employees to use the devices they are already own, thus reducing costs.

B. It should reduce the number of help desk and tickets significantly.

C. It is most secure, as the company owns and completely controls the devices.

D. It is the least complex method for systems administrator to maintain over time.

Correct Answer: A

QUESTION 4

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.

Correct Answer: C

Reference: https://www.cynet.com/network-attacks/network-attacks-and-network-security-threats/

QUESTION 5

After the latest risk assessment, the Chief Information Security Officer (CISO) decides to meet with the development and security teams to find a way to reduce the security task workload. The CISO would like to:

1.

Have a solution that uses API to communicate with other security tools.

2.

Use the latest technology possible.

3.

Have the highest controls possible on the solution.

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

A. EDR

B. CSP

C. SOAR

D. CASB

Correct Answer: C

QUESTION 6

Based on PCI DSS v3.4, One Particular database field can store data, but the data must be unreadable. Which of the following data objects meets this requirement?

A. PAN

B. CVV2

C. Cardholder name

D. expiration date

Correct Answer: A

QUESTION 7

When of the following is the BEST reason to implement a separation of duties policy?

A. It minimizes the risk of Dos due to continuous monitoring.

B. It eliminates the need to enforce least privilege by logging all actions.

C. It increases the level of difficulty for a single employee to perpetrate fraud.

D. it removes barriers to collusion and collaboration between business units.

Correct Answer: A

QUESTION 8

Following a successful exploitation of an RCE vulnerability during a penetration test, a systems administrator is performing remediation activities of the target system. Since the systems administrator was not involved in the planning process for the penetration test, a production server was inadvertently targeted and impacted by the actions of the penetration tester. Which of the following would be the most appropriate to reduce the impact of the penetration test in the future?

A. Leverage a purple team approach to refine scope definition.

B. Exclude non-production systems from the penetration test.

C. Implement a black-box approach for the penetration test.

D. Include an intercepting proxy in the production environment.

E. Rely on web application vulnerability scans instead of penetration testing.

Correct Answer: A

Purple teaming is a collaborative approach to cybersecurity that brings together red and blue teams to test and improve an organization\\'s security posture. The Purple Team is a combination of the Red and Blue Teams and work together to

identify and address vulnerabilities discovered in simulated attacks.

The White Team is typically made up of executive-level individuals who oversee and coordinate all of the other teams\\' efforts.

QUESTION 9

An architect is designing security scheme for an organization that is concerned about APTs. Any proposed architecture must meet the following requirements:

1.

Services must be able to be reconstituted quickly from a known-good state.

2.

Network services must be designed to ensure multiple diverse layers of redundancy.

3.

Defensive and responsive actions must be automated to reduce human operator demands.

Which of the following designs must be considered to ensure the architect meets these requirements? (Choose three.)

A. Increased efficiency by embracing advanced caching capabilities

B. Geographic distribution of critical data and services

C. Hardened and verified container usage

D. Emulated hardware architecture usage

E. Establishment of warm and hot sites for continuity of operations

F. Heterogeneous architecture

G. Deployment of IPS services that can identify and block malicious traffic

H. Implementation and configuration of a SOAR

Correct Answer: BEH

The designs that must be considered to ensure the architect meets these requirements are:

1.

Network services must be designed to ensure multiple diverse layers of redundancy.

2.

Establishment of warm and hot sites for continuity of operations.

Implementation and configuration of a SOAR (Security Orchestration, Automation and Response) system to automate defensive and responsive actions to reduce human operator demands.

Heterogeneous architecture refers to the use of different types of hardware and software in a system. It is not related to the design of network services to ensure multiple diverse layers of redundancy.

QUESTION 10

A security analyst is evaluating the security of an online customer banking system. The analyst has a 12-character password for the test account. At the login screen, the analyst is asked to enter the third, eighth, and eleventh characters of the password. Which of the following describes why this request is a security concern? (Choose two.)

A. The request is evidence that the password is more open to being captured via a keylogger.

B. The request proves that salt has not been added to the password hash, thus making it vulnerable to rainbow tables.

C. The request proves the password is encoded rather than encrypted and thus less secure as it can be easily reversed.

D. The request proves a potential attacker only needs to be able to guess or brute force three characters rather than 12 characters of the password.

E. The request proves the password is stored in a reversible format, making it readable by anyone at the bank who is given access.

F. The request proves the password must be in cleartext during transit, making it open to on-path attacks.

Correct Answer: DE

QUESTION 11

The Chief Information Security Officer (CISO) has outlined a five-year plan for the company that includes the following:

1.

Implement an application security program.

2.

Reduce the click rate on phishing simulations from 73% to 8%.

3.

Deploy EDR to all workstations and servers.

4.

Ensure all systems are sending logs to the SIEM.

5.

Reduce the percentage of systems with vulnerabilities from 89% to 5%.

Which of the following would BEST aid the CISO in determining whether these goals are obtainable?

A. An asset inventory

B. A third-party audit

C. A risk assessment

D. An organizational CMMI

Correct Answer: D

An organizational Capability Maturity Model Integration (CMMI) would best aid the CISO in determining whether these goals are obtainable. The CMMI is a process and behavioral model that helps organizations streamline process improvement and encourage behaviors that lead to improved performance.

By assessing the maturity of the organization\\'s processes and practices, the CMMI can help determine the feasibility of the CISO\\'s goals. It can identify strengths and weaknesses in the current approach, and suggest areas for improvement that would increase the likelihood of achieving the outlined goals.

While the other options (asset inventory, third-party audit, risk assessment) can provide valuable information and may be part of the overall strategy, they do not provide the comprehensive view of organizational capabilities offered by the CMMI.

QUESTION 12

An organization has an operational requirement with a specific equipment vendor. The organization is located in the United States, but the vendor is located in another region. Which of the following risks would be MOST concerning to the organization in the event of equipment failure?

A. Support may not be available during all business hours.

B. The organization requires authorized vendor specialists.

C. Each region has different regulatory frameworks to follow.

D. Shipping delays could cost the organization money.

Correct Answer: D

The question ask about immediate concerns for the organization would be the repair, replacement, or troubleshooting of the equipment to resume normal operations. Since the equipment is in another region, replacement would be a bigger concern than repairs. Delays in getting the required equipment or parts could result in prolonged downtime, impacting business operations and leading to financial losses.

QUESTION 13

An organization is working to secure its development process to ensure developers cannot deploy artifacts directly into the production environment. Which of the following security practice recommendations would be the best to accomplish this objective?

A. Implement least privilege access to all systems.

B. Roll out security awareness training for all users.

C. Set up policies and systems with separation of duties.

D. Enforce job rotations for all developers and administrators.

E. Utilize mandatory vacations for all developers.

F. Review all access to production systems on a quarterly basis.

Correct Answer: AC

QUESTION 14

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

Correct Answer: A

Reference: https://developer.arm.com/documentation/102433/0100/Stack-smashing-and-execution-permissions

QUESTION 15

DRAG DROP

A vulnerability scan with the latest definitions was performed across Sites A and B.

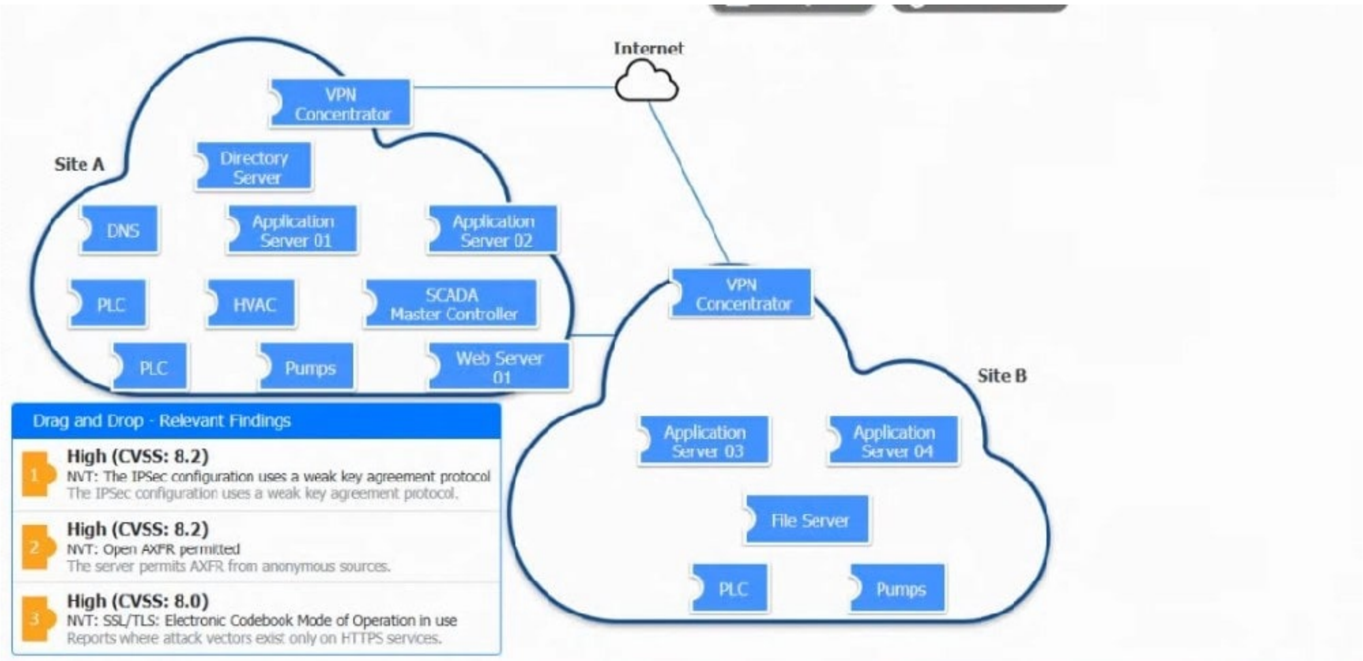
INSTRUCTIONS

Match each relevant finding to the affected host.

After associating the finding 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:



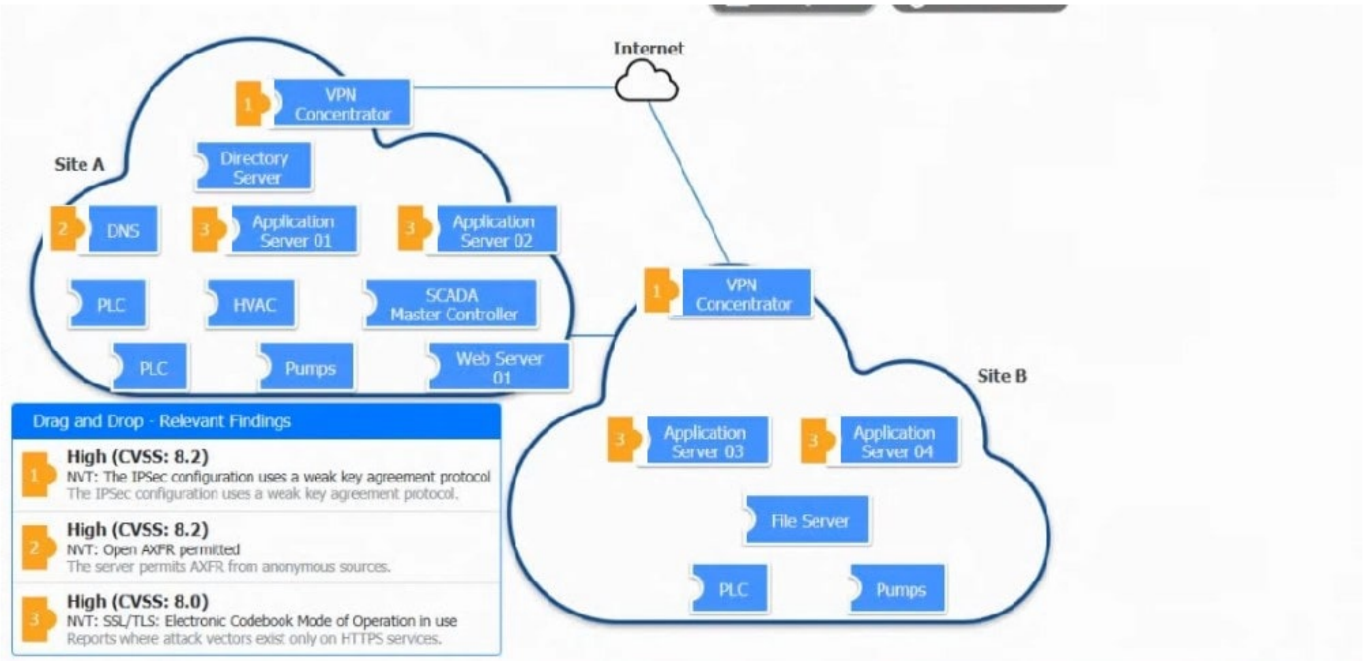
Drag and Drop - Relevant Findings

1 **High (CVSS: 8.2)**
NVT: The IPSec configuration uses a weak key agreement protocol
The IPSec configuration uses a weak key agreement protocol.

2 **High (CVSS: 8.2)**
NVT: Open AXFR permitted
The server permits AXFR from anonymous sources.

3 **High (CVSS: 8.0)**
NVT: SSL/TLS: Electronic Codebook Mode of Operation in use
Reports where attack vectors exist only on HTTPS services.

Correct Answer:



Drag and Drop - Relevant Findings

1 **High (CVSS: 8.2)**
NVT: The IPSec configuration uses a weak key agreement protocol
The IPSec configuration uses a weak key agreement protocol.

2 **High (CVSS: 8.2)**
NVT: Open AXFR permitted
The server permits AXFR from anonymous sources.

3 **High (CVSS: 8.0)**
NVT: SSL/TLS: Electronic Codebook Mode of Operation in use
Reports where attack vectors exist only on HTTPS services.

Latest CAS-004 Dumps CAS-004 PDF Dumps CAS-004 Study Guide