CAS-004^Q&As

CompTIA Advanced Security Practitioner (CASP+)

QUESTION 1

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 2

A company\\'s finance department acquired a new payment system that exports data to an unencrypted file on the system. The company implemented controls on the file so only appropriate personnel are allowed access. Which of the following risk techniques did the department use in this situation?

A. Accept

B. Avoid

C. Transfer

D. Mitigate

Correct Answer: D

QUESTION 3

To save time, a company that is developing a new VPN solution has decided to use the OpenSSL library within its proprietary software. Which of the following should the company consider to maximize risk reduction from vulnerabilities introduced by OpenSSL?

A. Include stable, long-term releases of third-party libraries instead of using newer versions.

B. Ensure the third-party library implements the TLS and disable weak ciphers.

C. Compile third-party libraries into the main code statically instead of using dynamic loading.

D. Implement an ongoing, third-party software and library review and regression testing.

Correct Answer: D

QUESTION 4

A global organization\\'s Chief Information Security Officer (CISO) has been asked to analyze the risks involved in a plan to move the organization\\'s current MPLS-based WAN network to use commodity internet and SD-WAN hardware. The SD-WAN provider is currently highly regarded but is a regional provider. Which of the following is MOST likely identified as a potential risk by the CISO?

A. The SD-WAN provider would not be able to handle the organization\\'s bandwidth requirements.

B. The operating costs of the MPLS network are too high for the organization.

C. The SD-WAN provider may not be able to support the required troubleshooting and maintenance.

D. Internal IT staff will not be able to properly support remote offices after the migration.

Correct Answer: C

QUESTION 5

A pharmaceutical company recently experienced a security breach within its customer-facing web portal. The attackers performed a SQL injection attack and exported tables from the company\\'s managed database, exposing customer information.

The company hosts the application with a CSP utilizing the IaaS model. Which of the following parties is ultimately responsible for the breach?

A. The pharmaceutical company

B. The cloud software provider

C. The web portal software vendor

D. The database software vendor

Correct Answer: A

QUESTION 6

Prior to a risk assessment inspection, the Chief Information Officer tasked the systems administrator with analyzing and reporting any configuration issues on the information systems, and then verifying existing security settings. Which of the following would be BEST to use?

A. SCAP

B. CVSS

C. XCCDF

D. CMDB

Correct Answer: A

QUESTION 7

An organization is looking to establish more robust security measures by implementing PKI. Which of the following should the security analyst implement when considering mutual authentication?

A. Perfect forward secrecy on both endpoints

B. Shared secret for both endpoints

C. Public keys on both endpoints

D. A common public key on each endpoint

E. A common private key on each endpoint

Correct Answer: C

QUESTION 8

A company is acquiring a competitor, and the security team is performing due diligence activities on the competitor prior to the acquisition. The team found a recent compliance audit of the competitor\\'s environment that shows a mature security infrastructure, but it lacks a cohesive policy and process framework. Based on the audit findings, the security team determines the competitor\\'s existing security capabilities are sufficient, but they will need to incorporate additional security policies. Which of the following risk management strategies is the security team recommending?

A. Mitigate and avoid

B. Transfer and accept

C. Avoid and transfer

D. Accept and mitigate

Correct Answer: D

The security team is accepting the risk that the competitor\\'s existing security policies and procedures are not comprehensive enough. However, the team is also mitigating this risk by implementing additional security policies.

QUESTION 9

A security engineer notices the company website allows users to select which country they reside in, such as the following example:

https://mycompany.com/main.php?Country=US

Which of the following vulnerabilities would MOST likely affect this site?

A. SQL injection

B. Remote file inclusion

C. Directory traversal

D. Unsecure references

Correct Answer: C

In a directory traversal attack, an attacker attempts to access files or directories that are located outside the web root directory or intended area. The URL parameter "Country=US" could potentially be manipulated by an attacker to traverse directories and access files they shouldn\\'t have access to.

QUESTION 10

Which of the following is the MOST important security objective when applying cryptography to control messages that tell an ICS how much electrical power to output?

A. Importing the availability of messages

B. Ensuring non-repudiation of messages

C. Enforcing protocol conformance for messages

D. Assuring the integrity of messages

Correct Answer: D

QUESTION 11

A security architect needs to implement a CASB solution for an organization with a highly distributed remote workforce. One Of the requirements for the implementation includes the capability to discover SaaS applications and block access to those that are unapproved or identified as risky. Which of the following would BEST achieve this objective?

A. Deploy endpoint agents that monitor local web traffic to enforce DLP and encryption policies.

B. Implement cloud infrastructure to proxy all user web traffic to enforce DI-P and encryption policies.

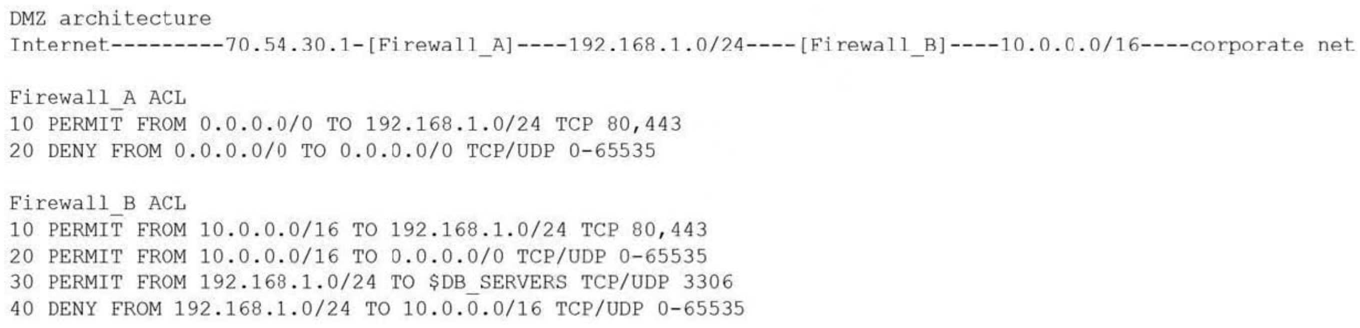
C. Implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy.

D. Deploy endpoint agents that monitor local web traffic and control access according to centralized policy.

Correct Answer: C

QUESTION 12

A security architect is reviewing the following proposed corporate firewall architecture and configuration:



```
DMZ architecture
Internet---------70.54.30.1-[Firewall_A]----192.168.1.0/24----[Firewall_B]----10.0.0.0/16----corporate net

Firewall_A ACL
10 PERMIT FROM 0.0.0.0/0 TO 192.168.1.0/24 TCP 80,443
20 DENY FROM 0.0.0.0/0 TO 0.0.0.0/0 TCP/UDP 0-65535

Firewall_B ACL
10 PERMIT FROM 10.0.0.0/16 TO 192.168.1.0/24 TCP 80,443
20 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
30 PERMIT FROM 192.168.1.0/24 TO $DB_SERVERS TCP/UDP 3306
40 DENY FROM 192.168.1.0/24 TO 10.0.0.0/16 TCP/UDP 0-65535
```

Both firewalls are stateful and provide Layer 7 filtering and routing. The company has the following requirements:

1.

Web servers must receive all updates via HTTP/S from the corporate network.

2.

Web servers should not initiate communication with the Internet.

3.

Web servers should only connect to preapproved corporate database servers.

4.

Employees\\' computing devices should only connect to web services over ports 80 and 443.

Which of the following should the architect recommend to ensure all requirements are met in the MOST secure manner? (Choose two.)

A. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP 80,443

B. Add the following to Firewall_A: 15 PERMIT FROM 192.168.1.0/24 TO 0.0.0.0 TCP 80,443

C. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535

D. Add the following to Firewall_B: 15 PERMIT FROM 0.0.0.0/0 TO 10.0.0.0/16 TCP/UDP 0-65535

E. Add the following to Firewall_B: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0 TCP/UDP 0-65535

F. Add the following to Firewall_B: 15 PERMIT FROM 192.168.1.0/24 TO 10.0.2.10/32 TCP 80,443

Correct Answer: AF

QUESTION 13

A company processes sensitive cardholder information that is stored in an internal production database and accessed by internet-facing web servers. The company\\'s Chief Information Security Officer (CISO) is concerned with the risks related to sensitive data exposure and wants to implement tokenization of sensitive information at the record level. The company implements a one-to-many mapping of primary credit card numbers to temporary credit card numbers.

Which of the following should the CISO consider in a tokenization system?

A. Data field watermarking

B. Field tagging

C. Single-use translation

D. Salted hashing

Correct Answer: C

QUESTION 14

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

Correct Answer: B

QUESTION 15

A company runs a well ttended, on-premises fitness club for its employees, about 200 of them each day. Employees want to sync center\\'s login and attendance program with their smartphones. Human resources, which manages the contract for the fitness center, has asked the security architecture to help draft security and privacy requirements.

Which of the following would BEST address these privacy concerns?

A. Use biometric authentication.

B. Utilize geolocation/geofencing.

C. Block unauthorized domain bridging.

D. Implement containerization

Correct Answer: A