CASP CAS-005 Practice Questions

Shared by Stephenson on 13-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An engineering team determines the cost to mitigate certain risks is higher than the asset values The team must ensure the risks are prioritized appropriately. Which of the following is the best way to address the issue?

Options:

A- Data labeling
B- Branch protection
C- Vulnerability assessments
D- Purchasing insurance

Answer:

D

Explanation:

When the cost to mitigate certain risks is higher than the asset values, the best approach is to purchase insurance. Thismethod allows the company to transfer the risk to an insurance provider, ensuring that financial losses are covered in the event of an incident. This approach is cost-effective and ensures that risks are prioritized appropriately without overspending on mitigation efforts.

CompTIA SecurityX Study Guide: Discusses risk management strategies, including risk transfer through insurance.

NIST Risk Management Framework (RMF): Highlights the use of insurance as a risk mitigation strategy.

'Information Security Risk Assessment Toolkit' by Mark Talabis and Jason Martin: Covers risk management practices, including the benefits of purchasing insurance.

Question 2

Question Type: MultipleChoice

A company wants to perform threat modeling on an internally developed, business-critical

application. The Chief Information Security Officer (CISO) is most concerned that the application should maintain 99.999% availability and authorized users should only be able to gain access to data they are explicitly authorized to view. Which of the following threat-modeling frameworks directly addresses the CISO's concerns about this system?

Options:

A- CAPEC
B- STRIDE
B- The permissions were not able to be migrated to the new system, and several stakeholders were made responsible for granting appropriate access.
C- ATT&CK
C- Pass-the-hash attack: This attack involves using a stolen hash of a user's password to authenticate without needing the actual password. It's unrelated to software package integrity.
Why A is the Correct Answer:
A supply chain attack is exactly what the organization is trying to mitigate. By creating a registry of known-good software packages and their hashes, they can verify that the packages they are using are legitimate and haven't been altered.
If an attacker were to compromise a software package in the supply chain, the hash of the altered package would not match the hash in the organization's registry. This would immediately alert the organization to a potential compromise.
CASP+ Relevance: This aligns with the CASP+ exam objectives, which emphasize the importance of risk management, threat intelligence, and implementing security controls to address various attack vectors, including supply chain risks.
How the Registry Works (Elaboration based on CASP+principles):
Hashing: When a package is vetted, a cryptographic hash function (like SHA-256) is used to generate a unique 'fingerprint' (the hash) of the package's contents.
Verification: Before installing or using a package, its hash is calculated and compared to the hash stored in the registry. A match confirms the package's integrity. A mismatch indicates tampering.
Incident Response: If a vulnerability is discovered in a commonly used package, the registry helps the organization quickly identify which systems are affected based on the dependency list and the stored hashes.
In conclusion, maintaining a registry of software dependencies with hashes is a crucial security control that directly addresses the threat of supply chain attacks by ensuring the integrity and authenticity of software packages. The use of hash functions for verification is a common practice in security and is emphasized in the CASP+ material.
D- TAXII
D- Perform threat modeling on the production application

Answer:

B, B

Question 3

Question Type: MultipleChoice

A security administrator needs to review the efficacy of the detection rules configured on the SIEM by employing real-world attacker TTPs. Which of the following actions should the security administrator take to accomplish this objective?

Options:

A- Perform an internal penetration test.
B- Use adversary emulation.
B- Create baseline images for each OS in use, following security standards, and integrate the images into the patching and deployment solution.
C- Execute an internal vulnerability assessment.
C- Review the application allow list on a daily basis to make sure it is properly configured.
D- Perform a threat hunt exercise.
D- improving security dashboard visualization on SIEM
E- Ingest new threat intelligence feeds.
E- {'name':'deployment', 'hosts':'linux_servers', 'remote_user':'Administrator', 'tasks':{'name':'Install security software', 'com.microsoft.store.latest'} }

Answer:

B, B

Explanation:

The best option is adversary emulation. Adversary emulation involves simulating real-world attacker Tactics, Techniques, and Procedures (TTPs) based on frameworks like MITRE ATT&CK. Unlike penetration tests, which primarily focus on identifying exploitable vulnerabilities, adversary emulation specifically tests the effectiveness of detection and response capabilities against known adversarial behaviors.

Option A (penetration testing) provides value but may not align test cases with SIEM detection rules. Option C (vulnerability assessment) identifies weaknesses but does not test detection rules. Option D (threat hunting) is proactive analysis but does not validate existing SIEM rule coverage in a structured manner. Option E (threat feeds) enrich SIEM data but do not test its efficacy.

CAS-005 identifies adversary emulation as a key strategy for validating detection and response coverage. It provides measurable results about what alerts are triggered and where detection gaps exist, enabling organizations to tune SIEM rules for improved efficacy.

Question 4

Question Type: MultipleChoice

A security administrator needs to review the efficacy of the detection rules configured on the SIEM by employing real-world attacker TTPs. Which of the following actions should the security administrator take to accomplish this objective?

Options:

A- Perform an internal penetration test.
B- Use adversary emulation.
B- Create baseline images for each OS in use, following security standards, and integrate the images into the patching and deployment solution.
C- Execute an internal vulnerability assessment.
C- Review the application allow list on a daily basis to make sure it is properly configured.
D- Perform a threat hunt exercise.
D- improving security dashboard visualization on SIEM
E- Ingest new threat intelligence feeds.
E- {'name':'deployment', 'hosts':'linux_servers', 'remote_user':'Administrator', 'tasks':{'name':'Install security software', 'com.microsoft.store.latest'} }

Answer:

B, B

Explanation:

The best option is adversary emulation. Adversary emulation involves simulating real-world attacker Tactics, Techniques, and Procedures (TTPs) based on frameworks like MITRE ATT&CK. Unlike penetration tests, which primarily focus on identifying exploitable vulnerabilities, adversary emulation specifically tests the effectiveness of detection and response capabilities against known adversarial behaviors.

Option A (penetration testing) provides value but may not align test cases with SIEM detection rules. Option C (vulnerability assessment) identifies weaknesses but does not test detection rules. Option D (threat hunting) is proactive analysis but does not validate existing SIEM rule coverage in a structured manner. Option E (threat feeds) enrich SIEM data but do not test its efficacy.

CAS-005 identifies adversary emulation as a key strategy for validating detection and response coverage. It provides measurable results about what alerts are triggered and where detection gaps exist, enabling organizations to tune SIEM rules for improved efficacy.

Question 5

Question Type: MultipleChoice

An organization is developing a disaster recovery plan that requires data to be backed up and available at a moment's notice. Which of the following should the organization consider first to address this requirement?

Options:

A- Implement a change management plan to ensure systems are using the appropriate versions.
B- Hire additional on-call staff to be deployed if an event occurs.
C- Design an appropriate warm site for business continuity.
D- Identify critical business processes and determine associated software and hardware requirements.

Answer:

D

Explanation:

For a disaster recovery (DR) plan requiring immediate data availability, the first step is understanding what needs to be protected and recovered. Identifying critical business processes and their associated software and hardware requirements establishes the foundation for the DR plan. This ensures that backups and recovery mechanisms align with business priorities, meeting the 'moment's notice' requirement.

Option A:A change management plan is important for system consistency but doesn't directly address immediate data availability in a DR context.

Option B:Hiring staff supports execution but doesn't define what needs to be recovered or how. It's a later step.

Option C:A warm site (a partially operational backup site) is a good DR solution, but designing it comes after identifying critical processes and resources.

Option D:This is the first step in any DR planning process---knowing what's critical ensures the plan meets availability goals efficiently.

Question 6

Question Type: MultipleChoice

A user reports application access issues to the help desk. The help desk reviews the logs for the user

Time	Internal IP	Public IP	IP geolocation	Application	Action
8:47 p.m.	192.168.1.5	104.18.16.29	Toronto	VPN	Allow
8:48 p.m.	10.10.2.21	95.67.137.12	Los Angeles	Email	Allow
8:48 p.m.	10.10.2.21	95.67.137.12	Los Angeles	Human resources system	Allow
8:49 p.m.	10.10.2.21	95.67.137.12	Los Angeles	Email	Allow
8:52 p.m.	192.168.1.5	104.18.16.29	Toronto	Human resources system	Deny

Which option best is most likely The reason for the issue?

Options:

A- The userinadvertently tripped the impossible travel security rule in the SSO system.
B- A threat actor has compromised the user's account and attempted to lop, m
C- The user is not allowed to access the human resources system outside of business hours
D- The user did not attempt to connect from an approved subnet

Answer:

A

Explanation:

Based on the provided logs, the user has accessed various applications from different geographic locations within a very short timeframe. This pattern is indicative of the 'impossible travel' security rule, a common feature in Single Sign-On (SSO) systems designed to detect and prevent fraudulent access attempts.

Analysis of Logs:

At 8:47 p.m., the user accessed a VPN from Toronto.

At 8:48 p.m., the user accessed email from Los Angeles.

At 8:48 p.m., the user accessed the human resources system from Los Angeles.

At 8:49 p.m., the user accessed email again from Los Angeles.

At 8:52 p.m., the user attempted to access the human resources system from Toronto, which was denied.

These rapid changes in location are physically impossible and typically trigger security measures to prevent unauthorized access. The SSO system detected these inconsistencies and likely flagged the activity as suspicious, resulting in access denial.

CompTIA SecurityX Study Guide

NIST Special Publication 800-63B, 'Digital Identity Guidelines'

'Impossible Travel Detection,' Microsoft Documentation

Question 7

Question Type: MultipleChoice

A security analyst is developing a threat model that focuses on attacks associated with the organization's storage products. The products:

* Are used in commercial and government user environments

* Are required to comply with crypto-export requirements

* Include both hardware and software components that are developed by external vendors in Europe and Asia

Which option best are the most important for the analyst to consider when developing the model? (Choose two).

Options:

A- Contractual obligations
B- Legal hold obligations
C- Trust boundaries
D- Cloud services enumeration
E- Supply chain access
F- Homomorphic encryption usage

Answer:

C, E

Explanation:

The most critical considerations are trust boundaries (C) and supply chain access (E). Trust boundaries define where sensitive data crosses between systems or organizations, requiring strict cryptographic protections---especially important in government and commercial environments subject to crypto-export controls.

Supply chain access is also critical because hardware and software are sourced from external vendors. If suppliers are compromised, attackers could introduce malicious code, backdoors, or tampered firmware, endangering customers worldwide.

Option A (contractual obligations) and B (legal hold) are compliance-related but not direct security threats. Option D (cloud services enumeration) is irrelevant unless the storage is cloud-based. Option F (homomorphic encryption) is an advanced technology but not required for base threat modeling.

CAS-005 highlights modeling adversary capabilities at trust boundaries and accounting for supply chain risks, making C and E the most important.