CAS-001Q&As

CompTIA Advanced Security Practitioner

QUESTION 1

The Information Security Officer (ISO) is reviewing a summary of the findings from the last COOP tabletop exercise. The Chief Information Officer (CIO) wants to determine which additional controls must be implemented to reduce the risk of an extended customer service outage due to the VoIP system being unavailable.

Which of the following BEST describes the scenario presented and the document the ISO is reviewing?

A. The ISO is evaluating the business implications of a recent telephone system failure within the BIA.

B. The ISO is investigating the impact of a possible downtime of the messaging system within the RA.

C. The ISO is calculating the budget adjustment needed to ensure audio/video system redundancy within the RFQ.

D. The ISO is assessing the effect of a simulated downtime involving the telecommunication system within the AAR.

Correct Answer: D

QUESTION 2

Which of the following does SAML uses to prevent government auditors or law enforcement from identifying specific entities as having already connected to a service provider through an SSO operation?

A. Transient identifiers

B. Directory services

C. Restful interfaces

D. Security bindings

Correct Answer: A

QUESTION 3

Wireless users are reporting issues with the company\\'s video conferencing and VoIP systems. The security administrator notices DOS attacks on the network that are affecting the company\\'s VoIP system (i.e. premature call drops and garbled call signals). The security administrator also notices that the SIP servers are unavailable during these attacks.

Which of the following security controls will MOST likely mitigate the VoIP DOS attacks on the network? (Select TWO).

A. Configure 802.11b on the network

B. Configure 802.1q on the network

C. Configure 802.11e on the network

D. Update the firewall managing the SIP servers

E. Update the HIDS managing the SIP servers

Correct Answer: CD

QUESTION 4

As part of the testing phase in the SDLC, a software developer wants to verify that an application is properly handling user error exceptions. Which of the following is the BEST tool or process for the developer use?

A. SRTM review

B. Fuzzer

C. Vulnerability assessment

D. HTTP interceptor

Correct Answer: B

QUESTION 5

A mid-level company is rewriting its security policies and has halted the rewriting progress because the company\\'s executives believe that its major vendors, who have cultivated a strong personal and professional relationship with the senior level staff, have a good handle on compliance and regulatory standards. Therefore, the executive level managers are allowing vendors to play a large role in writing the policy. Having experienced this type of environment in previous positions, and being aware that vendors may not always put the company\\'s interests first, the IT Director decides that while vendor support is important, it is critical that the company writes the policy objectively.

Which of the following is the recommendation the IT Director should present to senior staff?

A. 1) Consult legal, moral, and ethical standards; 2) Draft General Organizational Policy; 3) Specify Functional Implementing Policies; 4) Allow vendors to review and participate in the establishment of focused compliance standards, plans, and procedures

B. 1) Consult legal and regulatory requirements; 2) Draft General Organizational Policy; 3) Specify Functional Implementing Policies; 4) Establish necessary standards, procedures, baselines, and guidelines

C. 1) Draft General Organizational Policy; 2) Establish necessary standards and compliance documentation; 3) Consult legal and industry security experts; 4) Determine acceptable tolerance guidelines

D. 1) Draft a Specific Company Policy Plan; 2) Consult with vendors to review and collaborate with executives; 3) Add industry compliance where needed; 4) Specify Functional Implementing Policies

Correct Answer: B

QUESTION 6

The Chief Information Officer (CIO) of a technology company is likely to move away from a de- perimeterized model for employee owned devices. This is because there were too many issues with lack of patching, malware incidents, and data leakage due to lost/stolen devices which did not have full-disk encryption. The `bring your own computing\\' approach was originally introduced because different business units preferred different operating systems and application stacks.

Based on the issues and user needs, which of the following is the BEST recommendation for the CIO to make?

A. The de-perimeterized model should be kept as this is major industry trend and other companies are following this direction. Advise that the issues being faced are standard business as usual concerns in a modern IT environment.

B. Update the policy to disallow non-company end-point devices on the corporate network. Develop security-focused standard operating environments (SOEs) for all required operating systems and ensure the needs of each business unit are met.

C. The de-perimeterized model should be kept but update company policies to state that non- company end-points require full disk encryption, anti-virus software, and regular patching.

D. Update the policy to disallow non-company end-point devices on the corporate network. Allow only one type of outsourced SOE to all users as this will be easier to provision, secure, and will save money on operating costs.

Correct Answer: B

QUESTION 7

If a technician must take an employee\\'s workstation into custody in response to an investigation, which of the following can BEST reduce the likelihood of related legal issues?

A. A formal letter from the company\\'s president approving the seizure of the workstation.

B. A formal training and awareness program on information security for all company managers.

C. A screen displayed at log in that informs users of the employer\\'s rights to seize, search, and monitor company devices.

D. A printout of an activity log, showing that the employee has been spending substantial time on non-work related websites.

Correct Answer: C

QUESTION 8

An organization must comply with a new regulation that requires the organization to determine if an external attacker is able to gain access to its systems from outside the network. Which of the following should the company conduct to meet the regulation\\'s criteria?

A. Conduct a compliance review

B. Conduct a vulnerability assessment

C. Conduct a black box penetration test

D. Conduct a full system audit

Correct Answer: C

QUESTION 9

The company\\'s marketing department needs to provide more real-time interaction with its partners and consumers and decides to move forward with a presence on multiple social networking sites for sharing information. Which of the following minimizes the potential exposure of proprietary information?

A. Require each person joining the company\\'s social networking initiative to accept a non- disclosure agreement.

B. Establish a specific set of trained people that can release information on the organization\\'s behalf.

C. Require a confidential statement be attached to all information released to the social networking sites.

D. Establish a social media usage policy and provide training to all marketing employees.

Correct Answer: B

QUESTION 10

A security manager has started a new job and has identified that a key application for a new client does not have an accreditation status and is currently not meeting the compliance requirement for the contract\\'s SOW. The security manager has competing priorities and wants to resolve this issue quickly with a system determination and risk assessment.

Which of the following approaches presents the MOST risk to the security assessment?

A. The security manager reviews the system description for the previous accreditation, but does not review application change records.

B. The security manager decides to use the previous SRTM without reviewing the system description.

C. The security manager hires an administrator from the previous contract to complete the assessment.

D. The security manager does not interview the vendor to determine if the system description is accurate.

Correct Answer: B

QUESTION 11

An extensible commercial software system was upgraded to the next minor release version to patch a security vulnerability. After the upgrade, an unauthorized intrusion into the system was detected. The software vendor is called in to troubleshoot the issue and reports that all core components were updated properly.

Which of the following has been overlooked in securing the system? (Select TWO).

A. The company\\'s IDS signatures were not updated.

B. The company\\'s custom code was not patched.

C. The patch caused the system to revert to http.

D. The software patch was not cryptographically signed.

E. The wrong version of the patch was used.

F. Third-party plug-ins were not patched.

Correct Answer: BF

QUESTION 12

Statement: "The system shall implement measures to notify system administrators prior to a security incident occurring." Which of the following BEST restates the above statement to allow it to be implemented by a team of software developers?

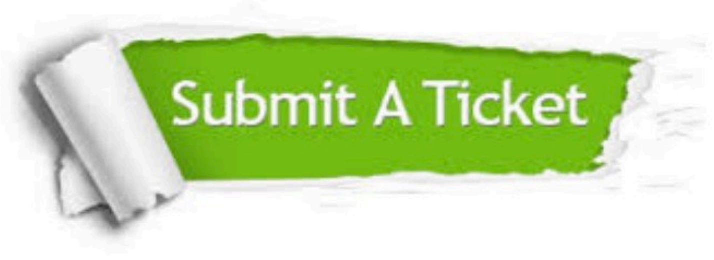
A. The system shall cease processing data when certain configurable events occur.

B. The system shall continue processing in the event of an error and email the security administrator the error logs.

C. The system shall halt on error.

D. The system shall throw an error when specified incidents pass a configurable threshold.

Correct Answer: D


Submit A Ticket

100%