Vendor: CompTIA

Exam Code:CAS-002

Exam Name: CompTIA Advanced Security Practitioner Exam

Version: Demo

QUESTION 1

The internal auditor at Company ABC has completed the annual audit of the company\\'s financial system. The audit report indicates that the accounts receivable department has not followed proper record disposal procedures during a COOP/ BCP tabletop exercise involving manual processing of financial transactions.

Which of the following should be the Information Security Officer\\'s (ISO\\'s) recommendation? (Select TWO).

A. Wait for the external audit results

B. Perform another COOP exercise

C. Implement mandatory training

D. Destroy the financial transactions

E. Review company procedures

Correct Answer: CE

QUESTION 2

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 3

An organization determined that each of its remote sales representatives must use a smartphone for email access.

The organization provides the same centrally manageable model to each person.

Which of the following mechanisms BEST protects the confidentiality of the resident data?

A. Require dual factor authentication when connecting to the organization\\'s email server.

B. Require each sales representative to establish a PIN to access the smartphone and limit email storage to two weeks.

C. Require encrypted communications when connecting to the organization\\'s email server.

D. Require a PIN and automatic wiping of the smartphone if someone enters a specific number of incorrect PINs.

Correct Answer: D

QUESTION 4

A new IT company has hired a security consultant to implement a remote access system, which will enable employees to telecommute from home using both company issued as well as personal computing devices, including mobile devices. The company wants a flexible system to provide confidentiality and integrity for data in transit to the company\\'s internally developed application GUI. Company policy prohibits employees from having administrative rights to company issued devices. Which of the following remote access solutions has the lowest technical complexity?

A. RDP server

B. Client-based VPN

C. IPSec

D. Jump box

E. SSL VPN

Correct Answer: A

QUESTION 5

A port in a fibre channel switch failed, causing a costly downtime on the company\\'s primary website. Which of the following is the MOST likely cause of the downtime?

A. The web server iSCSI initiator was down.

B. The web server was not multipathed.

C. The SAN snapshots were not up-to-date.

D. The SAN replication to the backup site failed.

Correct Answer: B

QUESTION 6

Wireless users are reporting issues with the company\\'s video conferencing and VoIP systems. The security administrator notices internal DoS attacks from infected PCs on the network causing the VoIP system to drop calls. 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. Install a HIPS on the SIP servers

B. Configure 802.1X on the network

C. Update the corporate firewall to block attacking addresses

D. Configure 802.11e on the network

E. Configure 802.1q on the network

Correct Answer: AD

QUESTION 7

A security auditor suspects two employees of having devised a scheme to steal money from the company. While one employee submits purchase orders for personal items, the other employee approves these purchase orders. The auditor has contacted the human resources director with suggestions on how to detect such illegal activities. Which of the following should the human resource director implement to identify the employees involved in these activities and reduce the risk of this activity occurring in the future?

A. Background checks

B. Job rotation

C. Least privilege

D. Employee termination procedures

Correct Answer: B

QUESTION 8

The latest independent research shows that cyber attacks involving SCADA systems grew an average of 15% per year in each of the last four years, but that this year\\'s growth has slowed to around 7%. Over the same time period, the number of attacks against applications has decreased or stayed flat each year. At the start of the measure period, the incidence of PC boot loader or BIOS based attacks was negligible. Starting two years ago, the growth in the number of PC boot loader attacks has grown exponentially. Analysis of these trends would seem to suggest which of the following strategies should be employed?

A. Spending on SCADA protections should stay steady; application control spending should increase substantially and spending on PC boot loader controls should increase substantially.

B. Spending on SCADA security controls should stay steady; application control spending should decrease slightly and spending on PC boot loader protections should increase substantially.

C. Spending all controls should increase by 15% to start; spending on application controls should be suspended, and PC boot loader protection research should increase by 100%.

D. Spending on SCADA security controls should increase by 15%; application control spending should increase slightly, and spending on PC boot loader protections should remain steady.

Correct Answer: B

QUESTION 9

A security administrator is tasked with increasing the availability of the storage networks while enhancing the performance of existing applications. Which of the following technologies should the administrator implement to meet these goals? (Select TWO).

A. LUN masking

B. Snapshots

C. vSAN

D. Dynamic disk pools

E. Multipath

F. Deduplication

Correct Answer: DE

QUESTION 10

A security administrator is redesigning, and implementing a service-oriented architecture to replace an old, in-house software processing system, tied to a corporate sales website. After performing the business process analysis, the administrator decides the services need to operate in a dynamic fashion. The company has also been the victim of data injection attacks in the past and needs to build in mitigation features. Based on these requirements and past vulnerabilities, which of the following needs to be incorporated into the SOA?

A. Point to point VPNs for all corporate intranet users.

B. Cryptographic hashes of all data transferred between services.

C. Service to service authentication for all workflows.

D. Two-factor authentication and signed code

Correct Answer: C

QUESTION 11

An accountant at a small business is trying to understand the value of a server to determine if the business can afford to buy another server for DR. The risk manager only provided the accountant with the SLE of $24,000, ARO of 20% and the exposure factor of 25%. Which of the following is the correct asset value calculated by the accountant?

A. $4,800

B. $24,000

C. $96,000

D. $120,000

Correct Answer: C

QUESTION 12

A company Chief Information Officer (CIO) is unsure which set of standards should govern the company\\'s IT policy.

The CIO has hired consultants to develop use cases to test against various government and industry security standards. The CIO is convinced that there is large overlap between the configuration checks and security controls governing each set of standards. Which of the following selections represent the BEST option for the CIO?

A. Issue a RFQ for vendors to quote a complete vulnerability and risk management solution to the company.

B. Issue a policy that requires only the most stringent security standards be implemented throughout the company.

C. Issue a policy specifying best practice security standards and a baseline to be implemented across the company.

D. Issue a RFI for vendors to determine which set of security standards is best for the company.

Correct Answer: C