CompTIA

CS0-002 Exam

CompTIA CySA+ Certification Exam

Questions & Answers
Demo

Version: 28.0

Question: 1

A Chief Executive Officer (CEO) is concerned about the company's intellectual property being leaked to competitors. The security team performed an extensive review but did not find any indication of an outside breach. The data sets are currently encrypted using the Triple Data Encryption Algorithm. Which of the following courses of action is appropriate?

A. Limit all access to the sensitive data based on geographic access requirements with strict role-based access controls.
B. Enable data masking and reencrypt the data sets using AES-256.
C. Ensure the data is correctly classified and labeled, and that DLP rules are appropriate to prevent disclosure.
D. Use data tokenization on sensitive fields, reencrypt the data sets using AES-256, and then create an MD5 hash.

Answer: B

Explanation:

Data masking is a technique that replaces sensitive data with fictitious but realistic data, thus preventing unauthorized access to the original data. Reencrypting the data sets using AES-256 would provide a stronger level of encryption than Triple DES, which has been deprecated by NIST due to its vulnerability to attacks12
Reference: 1 What Is AES-256 Encryption? How Does It Work? - MUO 2 Archived NIST Technical Series Publication

Question: 2

A company's Chief Information Security Officer (CISO) published an Internet usage policy that prohibits employees from accessing unauthorized websites. The IT department whitelisted websites used for business needs. The CISO wants the security analyst to recommend a solution that would improve security and support employee morale. Which of the following security recommendations would allow employees to browse non-business-related websites?

A. Implement a virtual machine alternative.
B. Develop a new secured browser.
C. Configure a personal business VLAN.
D. Install kiosks throughout the building.

Answer: A

Explanation:

A virtual machine alternative is a solution that allows employees to access non-business-related websites on a separate virtual machine that is isolated from the company's network and data. This way, the employees can browse the internet without compromising the security or performance of the company's systems3
Reference: 3 What is a virtual machine and how does it work? | Norton

Question: 3

In web application scanning, static analysis refers to scanning:

A. the system for vulnerabilities before installing the application.
B. the compiled code of the application to detect possible issues.
C. an application that is installed and active on a system.
D. an application that is installed on a system that is assigned a static IP.

Answer: B

Explanation:

This type of analysis is performed before the application is installed and active on a system, and it involves examining the code without actually executing it in order to identify potential vulnerabilities or security risks.

As per CYSA+ 002 Study Guide: Static analysis is conducted by reviewing the code for an application. Static analysis does not run the program; instead, it focuses on understanding how the program is written and what the code is intended to do.
Static analysis refers to scanning the source code or the compiled code of an application without executing it, to identify potential vulnerabilities, errors, or bugs. Static analysis can help improve the quality and security of the code before it is deployed or run4
Reference: 4 What Is Static Analysis? | Veracode

Question: 4

An organization has the following risk mitigation policy:
Risks with a probability of 95% or greater will be addressed before all others regardless of the impact.
All other prioritization will be based on risk value.
The organization has identified the following risks:

Risk	Probability	Impact
A	95%	$110,000
B	99%	$100,000
C	50%	$120,000
D	90%	$50,000

Which of the following is the order of priority for risk mitigation from highest to lowest?

A. A, B, D, C
B. A, B, C, D
C. D, A, B, C
D. D, A, C, B

Answer: D

Explanation:

According to the risk mitigation policy, risks with a probability of 95% or greater will be addressed first, regardless of the impact. Therefore, risk D is the highest priority, as it has a probability of 95% and an impact of $100,000. The next priority is risk A, which has a probability of 90% and an impact of $200,000. The remaining risks will be prioritized based on their risk value, which is calculated by multiplying the probability and the impact. Risk C has a risk value of $40,000 (80% x $50,000), while risk B has a risk value of $30,000 (60% x $50,000). Therefore, risk C is higher priority than risk B.

Question: 5

A security analyst is looking at the headers of a few emails that appear to be targeting all users at an organization:

From:	Justin OReilly
Subject:	Your tax documents is ready for secure download
Date:	2020-01-30
To:	sara.ellis@exampledomain.org
Return-Path:	justinoreilly@provider.com
Received From:	justing@sssofk12awq.com

From:	Justin OReilly
Subject:	Your tax documents is ready for secure download
Date:	2020-01-30
To:	jason.lee@exampledomain.org
Return-Path:	justinoreilly@provider.com
Received From:	justing@sssofk12awq.com

Which of the following technologies would MOST likely be used to prevent this phishing attempt?

A. DNSSEC
B. DMARC
C. STP
D. S/IMAP

Answer: B

Explanation:

DMARC stands for Domain-based Message Authentication, Reporting and Conformance. It is an email authentication protocol that helps prevent spoofing and phishing attacks by verifying that the sender's domain matches the domain in the email header. DMARC also provides a way for domain owners to specify how receivers should handle unauthenticated messages from their domain1

Reference: 1 What is DMARC? | DMARC.org