Free Questions for CS0-002 by actualtestdumps

Shared by Cleveland on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

industry partners from critical infrastructure organizations were victims of attacks on their SCADA devices. The attacks used privilege escalation to gain access to SCADA administration and access management solutions would help to mitigate this risk?

Options:

A- Multifactor authentication

B- Manual access reviews

C- Endpoint detection and response

D- Role-based access control

Answer:

A

Question 2

A security analyst is performing a Diamond Model analysis of an incident the company had last quarter. A potential benefit of this activity is that it can identify:

Options:

A- detection and prevention capabilities to improve.

B- which systems were exploited more frequently.

C- possible evidence that is missing during forensic analysis.

D- which analysts require more training.

E- the time spent by analysts on each of the incidents.

Answer:

A

Question 3

Question Type: **MultipleChoice**

A small business does not have enough staff in the accounting department to segregate duties. The controller writes the checks for the business and reconciles them against the ledger. To ensure there is no fraud occurring, the business conducts quarterly reviews in which a different officer in the business compares all the cleared checks against the ledger. Which of the following BEST describes this type of control?

Options:

A- Deterrent

B- Preventive

C- Compensating

D- Detective

Answer:

B

Question 4

Question Type: **MultipleChoice**

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: 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?

Options:

A- DNSSEC

B- DMARC

C- STP

D- S/IMAP

Answer:

B

Question 5

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?

Options:

A- A, B, D, C

B- A, B, C, D

C- D, A, B, C

D- D, A, C, B

Answer:

D

Question 6

Question Type: **MultipleChoice**

In web application scanning, static analysis refers to scanning:

Options:

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:

A

Question 7

Question Type: **MultipleChoice**

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?

Options:

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:

C