Free Questions for CS0-003 by certsdeals

Shared by Baird on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A healthcare organization must develop an action plan based on the findings from a risk

assessment. The action plan must consist of:

* Risk categorization

* Risk prioritization

. Implementation of controls

INSTRUCTIONS

Click on the audit report, risk matrix, and SLA expectations documents to review their

contents.

On the Risk categorization tab, determine the order in which the findings must be

prioritized for remediation according to the risk rating score. Then, assign a categorization to each risk.

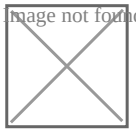
On the Controls tab, select the appropriate control(s) to implement for each risk finding.

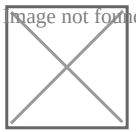
Findings may have more than one control implemented. Some controls may be used

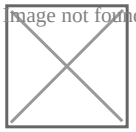
more than once or not at all.

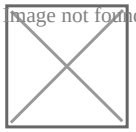
If at any time you would like to bring back the initial state of the simulation, please click

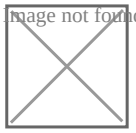
the Reset All button.











Options:

A) See the solution below in Explanation

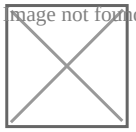
Answer:

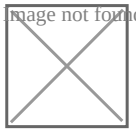
A

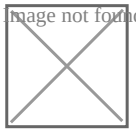
Question 2

Question Type: **MultipleChoice**

Approximately 100 employees at your company have received a Phishing email. AS a security analyst. you have been tasked with handling this Situation.





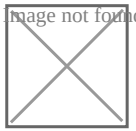


Review the information provided and determine the following:

1. HOW many employees Clicked on the link in the Phishing email?

2. on how many workstations was the malware installed?

3. what is the executable file name of the malware?



Options:

A) se ethe answer in explanation for thi stask

Answer:

A

Explanation:

1. How many employees clicked on the link in the phishing email?

According to the email server logs, 25 employees clicked on the link in the phishing email.

2. On how many workstations was the malware installed?

According to the file server logs, the malware was installed on 15 workstations.

3. What is the executable file name of the malware?

The executable file name of the malware is svchost.EXE.

Answers

1. 25

2. 15

3. svchost.EXE

Question 3

Question Type: **MultipleChoice**

Approximately 100 employees at your company have received a Phishing email. AS a security analyst. you have been tasked with handling this Situation.

Image not found or type unknown

Image not found or type unknown

Review the information provided and determine the following:

1. HOW many employees Clicked on the link in the Phishing email?

2. on how many workstations was the malware installed?

3. what is the executable file name of the malware?

Image not found or type unknown

Options:

A) se ethe answer in explanation for thi stask

Answer:

A

Explanation:

1. How many employees clicked on the link in the phishing email?

According to the email server logs, 25 employees clicked on the link in the phishing email.

2. On how many workstations was the malware installed?

According to the file server logs, the malware was installed on 15 workstations.

3. What is the executable file name of the malware?

The executable file name of the malware is svchost.EXE.

Answers

1. 25

2. 15

3. svchost.EXE

Question 4

Question Type: MultipleChoice

A security analyst is trying to detect connections to a suspicious IP address by collecting the packet captures from the gateway. Which of the following commands should the security analyst consider running?

A grep [IP address] packets.pcap

B cat packets.pcap | grep [IP Address]

Options:

C) tcpdump -n -r packets.pcap host [IP address]

D) strings packets.pcap | grep [IP Address]

Answer:

C

Explanation:

tcpdump is a command-line tool that can capture and analyze network packets from a given interface or file. The -n option prevents tcpdump from resolving hostnames, which can speed up the analysis. The -r option reads packets from a file, in this case packets.pcap. The host [IP address] filter specifies that tcpdump should only display packets that have the given IP address as either the source or the destination. This command can help the security analyst detect connections to a suspicious IP address by collecting the packet captures from the gateway. Official Reference:

https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives

https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-CySA-test-questions-with-answers

https://www.reddit.com/r/CompTIA/comments/tmxx84/passed_cysa_heres_my_experience_and_how_i_studied/

Question 5

Question Type: **MultipleChoice**

A healthcare organization must develop an action plan based on the findings from a risk

assessment. The action plan must consist of:

* Risk categorization

* Risk prioritization

. Implementation of controls

INSTRUCTIONS

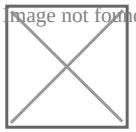
Click on the audit report, risk matrix, and SLA expectations documents to review their

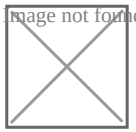
contents.

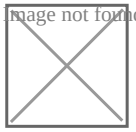
On the Risk categorization tab, determine the order in which the findings must be prioritized for remediation according to the risk rating score. Then, assign a categorization to each risk.

On the Controls tab, select the appropriate control(s) to implement for each risk finding. Findings may have more than one control implemented. Some controls may be used more than once or not at all.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.







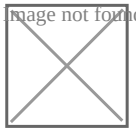
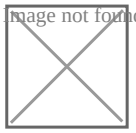


Image not found or type unknown



Options:

A) See the solution below in Explanation

Answer:

A