

Free Questions for CIS-VR by certsinside

Shared by Harrison on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is the best way to develop a complete list of Vulnerability Reports?

Options:

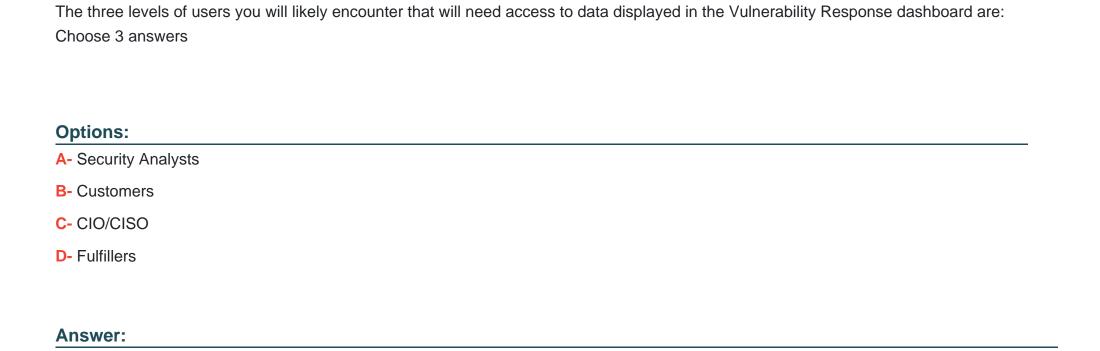
- A- Recommend that the client purchase the full Performance Analytics package.
- B- Ask the CISO.
- C- Work with the customer to identify the things that will be most useful to them.
- D- Use the standard out of the box reports only.

Answer:

В

Question 2

Question Type: MultipleChoice



Question 3

Α

Question Type: MultipleChoice

What type of data would the CIO/CISO want on the dashboard?

Options:
A- Aggregations for priority and workload
B- Drill-down to granularity
C- Single, clear indicators of organizational health
D- Up to the minute views
Answer:
A
Question 4
Question Type: MultipleChoice
Which of the following best describes the Vulnerable item State Approval Workflow?

A- It is read-only, you can only change the Assignment Group members for the approval

Options:

- B- It exists in the Security Operations Common scope so it can be modified by any Security Operations AdminC- It can only be modified by System Adminstrators
- D- It runs against the [sn_vul_change_approval] table

Answer:

C

Question 5

Question Type: MultipleChoice

What is the ServiceNow application used for process automation?

Options:

- A- Knowledge Base
- **B-** Workflows
- C- SLAs
- **D-** Service Catalog

Question 6		
uestion Typ	e: MultipleChoice	
Which of th	e following is a common Integration point between Vulnerability and GRC?	
Options:		
	Incident Response	
B- Change		
C- Problem		
	cators	
D- Risk Ind		

Question 7

Question Type: MultipleChoice

A common Integration point with Vulnerability is:

Options:

- A- Workflow Mappings
- **B-** Risk Indicators within GRC
- **C-** Service Catalog
- D- Knowledge Base

Answer:

Α

Question 8

Question Type: MultipleChoice

If fixing a Vulnerable Item outweighs the benefits, the correct course of action is:

Options:

- A- Mark the CI inactive in the CMDB and notify the CI owner
- B- Record the accepted risk and Close/Defer the Vulnerable Item
- C- Deprioritize the Vulnerable item Records (VIT) to push them further down the list so it can be ignored
- D- Add the CI to the Vulnerability Scanners exclusions Related List

Answer:

Α

To Get Premium Files for CIS-VR Visit

https://www.p2pexams.com/products/cis-vr

For More Free Questions Visit

https://www.p2pexams.com/servicenow/pdf/cis-vr

