CertsCare

Free Questions for CIS-SIR by certscare

Shared by Waters on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Which Table would be commonly used for Security Incident Response?

Options:

A- sysapproval_approver

B- sec_ops_incident

C- cmdb_rel_ci

D- sn_si_incident

Answer:

D

Question 2

Question Type: **MultipleChoice**

Select the one capability that retrieves a list of running processes on a CI from a host or endpoint.

Options:

A- Get Network Statistics

B- Isolate Host

C- Get Running Processes

D- Publish Watchlist

E- Block Action

F- Sightings Search

Answer:

C

Question 3

Question Type: MultipleChoice

What is the fastest way for security incident administrators to remove unwanted widgets from the Security Incident Catalog?

Options:

A- Clicking the X on the top right corner

B- Talking to the system administrator

C- Can't be removed

D- Through the Catalog Definition record

Answer:

D

Question 4

Question Type: MultipleChoice

Which improvement opportunity can be found baseline which can contribute towards process maturity and strengthen costumer's overall security posture?

Options:

A- Post-Incident Review

B- Fast Eradication

C- Incident Containment

D- Incident Analysis

Answer:

D

Question 5

Question Type: **MultipleChoice**

What three steps enable you to include a new playbook in the Selected Playbook choice list? (Choose three.)

Options:

A- Add the TLP: GREEN tag to the playbooks that you want to include in the Selected Playbook choice list

B- Navigate to the sys_hub_flow.list table

C- Search for the new playbook you have created using Flow Designer

D- Add the sir_playbook tag to the playbooks that you want to include in the Selected Playbook choice list

E- Navigate to the sys_playbook_flow.list table

Answer:

B, C, D

Question 6

Question Type: **MultipleChoice**

What are two of the audiences identified that will need reports and insight into Security Incident Response reports? (Choose two.)

Options:

A- Analysts

B- Vulnerability Managers

C- Chief Information Security Officer (CISO)

D- Problem Managers

Answer:

A, B

Question 7

Question Type: MultipleChoice

The Risk Score is calculated by combining all the weights using .

Options:

A- an arithmetic mean

B- addition

C- the Risk Score script include

D- a geometric mean

Answer:

A

Question 8

Question Type: MultipleChoice

The severity field of the security incident is influenced by what?

Options:

A- The cost of the response to the security breach

B- The impact, urgency and priority of the incident

C- The time taken to resolve the security incident

D- The business value of the affected asset

Answer:

D

Question 9

Question Type: MultipleChoice

The following term is used to describe any observable occurrence: .

Options:

A- Incident

B- Log

C- Ticket

D- Alert

E- Event

Answer:

E

Question 10

Question Type: **MultipleChoice**

What is the purpose of Calculator Groups as opposed to Calculators?

Options:

A- To provide metadata about the calculators

B- To allow the agent to select which calculator they want to execute

C- To set the condition for all calculators to run

D- To ensure one at maximum will run per group

Answer:

C

To Get Premium Files for CIS-SIR Visit

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

For More Free Questions Visit

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

20%
DISCOUNT