Free Questions for CIS-SIR by dumpssheet

Shared by Owen on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What makes a playbook appear for a Security Incident if using Flow Designer?

Options:

A- Actions defined to create tasks

B- Trigger set to conditions that match the security incident

C- Runbook property set to true

D- Service Criticality set to High

Answer:

B

Question 2

Question Type: MultipleChoice

A flow consists of one or more actions and a what?

Options:

A- Change formatter

B- Catalog Designer

C- NIST Ready State

D- Trigger

Answer:

D

Question 3

Question Type: **MultipleChoice**

The EmailUserReportedPhishing script include processes inbound emails and creates a record in which table?

Options:

A- ar_sn_si_phishing_email

B- sn_si_incident

C- sn_si_phishing_email_header

D- sn_si_phishing_email

Answer:

A

Question 4

Question Type: **MultipleChoice**

Which of the following process definitions allow only single-step progress through the process defined without allowing step skipping?

Options:

A- SANS Stateful

B- NIST Stateful

C- SANS Open

D- NIST Open

Answer:

B

Question 5

Question Type: MultipleChoice

When the Security Phishing Email record is created what types of observables are stored in the record?

(Choose three.)

Options:

A- URLs, domains, or IP addresses appearing in the body

B- Who reported the phishing attempt

C- State of the phishing email

D- IP addresses from the header

E- Hashes and/or file names found in the EML attachment

F- Type of Ingestion Rule used to identify this email as a phishing attempt

Answer:

A, D, E

Question 6

Question Type: MultipleChoice

Security tag used when a piece of information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

Options:

A- TLP:GREEN

B- TLP:AMBER

C- TLP:RED

D- TLP:WHITE

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organizations	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to
TLP:GREEN Limited disclosure, restricted to the community	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules.	TLP:WHITE information may be distributed without restriction.

Answer:

B

Question 7

Question Type: MultipleChoice

Knowledge articles that describe steps an analyst needs to follow to complete Security incident tasks might be associated to those tasks through which of the following?

Options:

A- Work Instruction Playbook

B- Flow

C- Workflow

D- Runbook

E- Flow Designer

Answer:

D

Question 8

Question Type: MultipleChoice

What field is used to distinguish Security events from other IT events?

Options:

A- Type

B- Source

C- Classification

D- Description

Answer:

C

Question 9

Question Type: MultipleChoice

Which of the following fields is used to identify an Event that is to be used for Security purposes?

Options:

A- IT

B- Classification

C- Security

D- CI

Answer:

B

Question 10

Question Type: MultipleChoice

Joe is on the SIR Team and needs to be able to configure Territories and Skills. What role does he need?

Options:

A- Security Basic

B- Manager

C- Security Analyst

D- Security Admin

Answer:

D

Question 11

Question Type: **MultipleChoice**

What is the first step when creating a security Playbook?

Options:

A- Set the Response Task's state

B- Create a Flow

C- Create a Runbook

D- Create a Knowledge Article

Answer:

B

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