Free Questions for CIS-SIR by vceexamstest

Shared by Hall on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

This type of integration workflow helps retrieve a list of active network connections from a host or endpoint, so it can be used to enrich incidents during investigation.

Options:

A- Security Incident Response -- Get Running Services

B- Security Incident Response -- Get Network Statistics

C- Security Operations Integration -- Sightings Search

D- Security Operations Integration -- Block Request

Answer:

B

Question 2

Question Type: MultipleChoice

The benefits of improved Security Incident Response are expressed .

Options:

A- as desirable outcomes with clear, measurable Key Performance Indicators

B- differently depending upon 3 stages: Process Improvement, Process Design, and Post Go-Live

C- as a series of states with consistent, clear metrics

D- as a value on a scale of 1-10 based on specific outcomes

Answer:

C

Question 3

Question Type: **MultipleChoice**

What plugin must be activated to see the New Security Analyst UI?

Options:

A- Security Analyst UI Plugin

B- Security Incident Response UI plugin

C- Security Operations UI plugin

D- Security Agent UI Plugin

Answer:

D

Question 4

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 5

Question Type: **MultipleChoice**

What factor, if any, limits the ability to close SIR records?

Options:

A- Opened related INC records

B- Best practice dictates that SIR records should be set to 'Resolved' never to 'Closed'

C- Nothing, SIR records could be closed at any time

D- All post-incident review Question:ers have to be completed first

Answer:

A

Question 6

Question Type: MultipleChoice

Select the one capability that restricts connections from one CI to other devices.

Options:

A- Isolate Host

B- Sightings Search

C- Block Action

D- Get Running Processes

E- Get Network Statistics

F- Publish Watchlist

Answer:

A

Question 7

Question Type: **MultipleChoice**

What parts of the Security Incident Response lifecycle is responsible for limiting the impact of a security incident?

Options:

A- Post Incident Activity

B- Detection & Analysis

C- Preparation and Identification

D- Containment, Eradication, and Recovery

Answer:

D

Question 8

Question Type: MultipleChoice

If the customer's email server currently has an account setup to report suspicious emails, then what happens next?

Options:

A- an integration added to Exchange keeps the ServiceNow platform in sync

B- the ServiceNow platform ensures that parsing and analysis takes place on their mail server

C- the customer's systems are already handling suspicious emails

D- the customer should set up a rule to forward these mails onto the ServiceNow platform

Answer:

D

Question 9

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 10

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 11

Question Type: **MultipleChoice**

What does a flow require?

Options:

A- Security orchestration flows

B- Runbooks

C- CAB orders

D- A trigger

Answer:

D