CIS-SIR^{Q&As}

Certified Implementation Specialist - Security Incident Response

Pass ServiceNow CIS-SIR Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/cis-sir.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by ServiceNow Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

How do you select which process definition to use?

A. By selecting the desired process within the Process Definition module

B. By selecting the desired process within the Process Selection module

C. By setting the process definition record to Active

D. By setting the Script Include record to Active

Correct Answer: B

Reference: https://docs.servicenow.com/bundle/paris-security- management/page/product/security-incident-response/reference/setup-assistant- reference.html

QUESTION 2

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

A. Isolate Host

B. Sightings Search

C. Block Action

D. Get Running Processes

E. Get Network Statistics

F. Publish Watchlist

Correct Answer: A

Reference: https://docs.servicenow.com/bundle/paris-security- management/page/product/security-incident-response/task/perform-addtl-tasks-on-si.html

QUESTION 3

What does a flow require?

A. Security orchestration flows

B. Runbooks

C. CAB orders

D. A trigger

Correct Answer: D

QUESTION 4

What is the first step when creating a security Playbook?

A. Set the Response Task\\'s state

B. Create a Flow

C. Create a Runbook

D. Create a Knowledge Article

Correct Answer: B

QUESTION 5

A pre-planned response process contains which sequence of events?

A. Organize, Analyze, Prioritize, Contain

B. Organize, Detect, Prioritize, Contain

C. Organize, Prepare, Prioritize, Contain

D. Organize, Verify, Prioritize, Contain

Correct Answer: A

QUESTION 6

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

A. Security Basic

B. Manager

C. Security Analyst

D. Security Admin

Correct Answer: D

Reference: https://docs.servicenow.com/bundle/quebec-security- management/page/product/security-incident-response/reference/installed-with-sir.html

QUESTION 7

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

A. Post Incident Activity

B. Detection and Analysis

C. Preparation and Identification

D. Containment, Eradication, and Recovery

Correct Answer: D

Reference: https://searchsecurity.techtarget.com/definition/incident-response

QUESTION 8

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

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

Correct Answer: C

Reference: https://docs.servicenow.com/bundle/paris-security- management/page/product/security-incident-response/reference/setup-assistant- reference.html

QUESTION 9

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

A. Analysts

B. Vulnerability Managers

C. Chief Information Security Officer (CISO)

D. Problem Managers

Correct Answer: AB

Reference: https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc- type/resource- center/data-sheet/ds-security-operations.pdf

QUESTION 10

When the Security Phishing Email record is created what types of observables are stored in the record? (Choose three.)

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

Correct Answer: ADE

Reference: https://docs.servicenow.com/bundle/paris-security- management/page/product/security-incident-response/concept/sighting-searches-on- phishing-attacks.html

[CIS-SIR PDF Dumps](#)   [CIS-SIR VCE Dumps](#)   [CIS-SIR Braindumps](#)