CIS-SIR Q&As

Certified Implementation Specialist - Security Incident Response

Pass ServiceNow CIS-SIR Exam with 100% Guarantee

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

QUESTION 1

Why is it important that the Platform (System) Administrator and the Security Incident administrator role be separated? (Choose three.)

A. Access to security incident data may need to be restricted

B. Allow SIR Teams to control assignment of security roles

C. Clear separation of duty

D. Reduce the number of incidents assigned to the Platform Admin

E. Preserve the security image in the company

Correct Answer: BCD

QUESTION 2

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

A. Get Network Statistics

B. Isolate Host

C. Get Running Processes

D. Publish Watchlist

E. Block Action

F. Sightings Search

Correct Answer: C

Reference: https://docs.servicenow.com/bundle/quebec-security- management/page/product/security- operations-common/concept/get-running-processes- capability.html

QUESTION 3

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

A. Change formatter

B. Catalog Designer

C. NIST Ready State

D. Trigger

Correct Answer: D

Reference: https://docs.servicenow.com/bundle/quebec-servicenow- platform/page/administer/flow-designer/concept/flows.html

QUESTION 4

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 5

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

A. Incident

B. Log

C. Ticket

D. Alert

E. Event

Correct Answer: E