CIS-SIR$^{Q\&As}$

Certified Implementation Specialist - Security Incident Response

Pass ServiceNow CIS-SIR Exam with 100% Guarantee

QUESTION 1

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

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

Correct Answer: D

Reference: https://docs.servicenow.com/bundle/paris-security- management/page/product/security-incident-response/concept/urp-about.html

QUESTION 2

If a desired pre-built integration cannot be found in the platform, what should be your next step to find a certified integration?

A. Build your own through the REST API Explorer

B. Ask for assistance in the community page

C. Download one from ServiceNow Share

D. Look for one in the ServiceNow Store

Correct Answer: D

QUESTION 3

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 4

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 5

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

A. Type

B. Source

C. Classification

D. Description

Correct Answer: C

Reference: https://docs.servicenow.com/bundle/paris-security- management/page/product/security-incident-response/concept/c_ScIncdUseAlrts.html