

# CIS-SIR<sup>Q&As</sup>

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**

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-incidentresponse/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

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

2024 Latest leads4pass CIS-SIR PDF and VCE dumps Download

#### **QUESTION 4**

Select the one capability that restricts connections from one CI to other de	evices.
--	---------

- 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

 $Reference: https://docs.servicenow.com/bundle/paris-security- management/page/product/security-incident-response/concept/c\_ScIncdUseAIrts.html \\$ 

CIS-SIR Practice Test

CIS-SIR Exam Questions

**CIS-SIR Braindumps**