

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.pass2lead.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

Which improvement opportunity can be found baseline which can contribute towards process maturity and strengthen customer's overall security posture?

- A. Post-Incident Review
- B. Fast Eradication
- C. Incident Containment
- D. Incident Analysis

Correct Answer: D

QUESTION 2

The severity field of the security incident is influenced by what?

- A. The cost of the response to the security breach
- B. The impact, urgency and priority of the incident
- C. The time taken to resolve the security incident
- D. The business value of the affected asset

Correct Answer: D

QUESTION 3

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 4

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 5

A flow consists of. (Choose two.)

- A. Scripts
- B. Actions
- C. Processes
- D. Actors
- E. Triggers

Correct Answer: BE

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

QUESTION 6

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

QUESTION 7

To configure Security Incident Escalations, you need the following role(s):.

- A. sn_si.admin
- B. sn_si.admin or sn_si.manager
- C. sn_si.admin or sn_si.ciso
- D. sn_si.manager or sn_si.analyst

Correct Answer: A

Reference: <https://docs.servicenow.com/bundle/paris-security-management/page/product/security-incident-response/task/escalate-security-incident.html>

QUESTION 8

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 9

What makes a playbook appear for a Security Incident if using Flow Designer?

- A. Actions defined to create tasks
- B. Trigger set to conditions that match the security incident
- C. Runbook property set to true
- D. Service Criticality set to High

Correct Answer: B

QUESTION 10

Which one of the following reasons best describes why roles for Security Incident Response (SIR) begin with "sn_si"?

- A. Because SIR is a scoped application, roles and script includes will begin with the sn_si prefix
- B. Because the Security Incident Response application uses a Secure Identity token
- C. Because ServiceNow checks the instance for a Secure Identity when logging on to this scoped application
- D. Because ServiceNow tracks license use against the Security Incident Response Application

Correct Answer: B

[Latest CIS-SIR Dumps](#)

[CIS-SIR VCE Dumps](#)

[CIS-SIR Exam Questions](#)