



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.geekcert.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

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

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 3

Knowledge articles that describe steps an analyst needs to follow to complete Security incident tasks might be associated to those tasks through which of the following?

- A. Work Instruction Playbook
- B. Flow
- C. Workflow
- D. Runbook
- E. Flow Designer

Correct Answer: D

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



QUESTION 4

What specific role is required in order to use the REST API Explorer?

- A. admin
- B. sn_si.admin
- C. rest_api_explorer
- D. security_admin

Correct Answer: AC

Reference: [https://developer.servicenow.com/dev.do#!/learn/learning-plans/orlando/technology_partner_program/app_store_learnv2_rest_orlando_introduction_to_the_rest_a pi_explorer](https://developer.servicenow.com/dev.do#!/learn/learning-plans/orlando/technology_partner_program/app_store_learnv2_rest_orlando_introduction_to_the_rest_api_explorer)

QUESTION 5

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 VCE Dumps](#)

[CIS-SIR Practice Test](#)

[CIS-SIR Exam Questions](#)